THOMSON

MACHINE-ASSISTED TRANSLATION (MAT):

(19)【発行国】 日本国特許庁（ＪＰ）	**(19)[ISSUING COUNTRY]** Japan Patent Office (JP)
(12)【公報種別】 公開特許公報（Ａ）	**(12)[GAZETTE CATEGORY]** Laid-open Kokai Patent (A)
(11)【公開番号】 特開 2000-216774(P2000-216774A)	**(11)[KOKAI NUMBER]** Unexamined Japanese Patent 2000-216774(P2000-216774A)
(43)【公開日】 平成１２年８月４日（２０００．８．４）	**(43)[DATE OF FIRST PUBLICATION]** August 4, Heisei 12 (2000. 8.4)
(54)【発明の名称】 暗号文検証方法、そのプログラム記録媒体、及びその装置	**(54)[TITLE OF THE INVENTION]** The cryptogram verification method, its program recording medium, and its apparatus
(51)【国際特許分類第７版】 H04L 9/32 G09C 1/00 640	**(51)[IPC INT. CL. 7]** H04L 9/32 G09C 1/00 640
【ＦＩ】 H04L 9/00 675 D G09C 1/00 640 C	**[FI]** H04L 9/00 675 D G09C 1/00 640 C
【審査請求】 未請求	**[REQUEST FOR EXAMINATION]** No
【請求項の数】 ３３	**[NUMBER OF CLAIMS]** 33
【出願形態】 ＯＬ	**[FORM OF APPLICATION]** Electronic

【全頁数】　２１

(21)【出願番号】
特願平 11-15409

(22)【出願日】
平成１１年１月２５日（１９９９．１．２５）

(71)【出願人】

【識別番号】
000004226

【氏名又は名称】
日本電信電話株式会社

【住所又は居所】

(72)【発明者】

【氏名】
阿部　正幸

【住所又は居所】

(74)【代理人】

【識別番号】
100066153

【弁理士】

【氏名又は名称】

[NUMBER OF PAGES] 21

(21)[APPLICATION NUMBER]
Japanese Patent Application Heisei 11-15409

(22)[DATE OF FILING]
January 25, Heisei 11 (1999. 1.25)

(71)[PATENTEE/ASSIGNEE]

[ID CODE]
000004226

[NAME OR APPELLATION]
Nippon Telegraph and Telephone CORP.

[ADDRESS OR DOMICILE]

(72)[INVENTOR]

[NAME OR APPELLATION]
Abe　Masayuki

[ADDRESS OR DOMICILE]

(74)[AGENT]

[ID CODE]
100066153

[PATENT ATTORNEY]

[NAME OR APPELLATION]

草野　卓　（外１名）

Kusano Takashi　(and 1 other)

【テーマコード（参考）】
5J104

[THEME CODE (REFERENCE)]
5J104

【Ｆターム（参考）】
5J104 AA01 AA08 JA23 JA29 LA00 LA03 LA05 LA06 NA02 NA08 NA12 NA18

[F TERM (REFERENCE)]
5J104 AA01 AA08 JA23 JA29 LA00 LA03 LA05 LA06 NA02 NA08 NA12 NA18

(57)【要約】

(57)[ABSTRACT OF THE DISCLOSURE]

【課題】
検証式における値に関する情報を漏らすことなく、暗号文の正当性の有無を示すことができる。

[SUBJECT OF THE INVENTION]
The existence of the correctness of a cryptogram can be shown without leaking the information about the value in a verification type.

【解決手段】
ｐは大きな素数、ｑはｐ－１を割り切る大きな素数とし、Ｇｑの元ｇ１，ｇ２を任意に選択し、$X=g1^{x1}g2^{x2} \bmod p$，$Y=g1^{y1}g2^{y2} \bmod p$，$Z=g1^{z} \bmod p$を暗号化に用いる公開鍵とし、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）$\in Zq^5$を秘密鍵とし、平文ｍの暗号文Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を受信し（Ｓ１）、乱数ｒを生成し（Ｓ２）、ｃ＝Ｈ（ｕ１，ｕ２）、$V=(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r} \bmod p$を計算し（Ｓ３）、Ｖ＝１なら暗号文を合格として復号し、不合格なら零知識証明により、ｒ，ｘ１，

[PROBLEM TO BE SOLVED]
It considers it as the big prime number among which p gives a clear-cut solution to a big prime number, and q gives p-1, and chooses the origin g1 and g2 of Gq as desired, let $X=g1^{x1}g2^{x2} \bmod p$, $Y=g1^{y1}g2^{y2} \bmod p$, $Z=g1^{z} \bmod p$ be the public key which it uses for encryption, let $(x1,x2,y1,y2,z)(\text{element of})Zq^5$ be a secret key, it receives cryptogram E= (u1, u2, v, e) of Plaintext m.
(S1), it forms a random number r.
(S2), c=H (u1, u2), v= (calculating $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r} \bmod p$)
(S3), if it is V= 1, it decodes a cryptogram as a pass, if it is a rejection, it proves that it is a rejection by zero knowledge proof, without leaking a function secret to r, x1, x2, y1, and y2.

ｘ２，ｙ１，ｙ２に関数秘密を漏らさずに不合格であることを証明する。

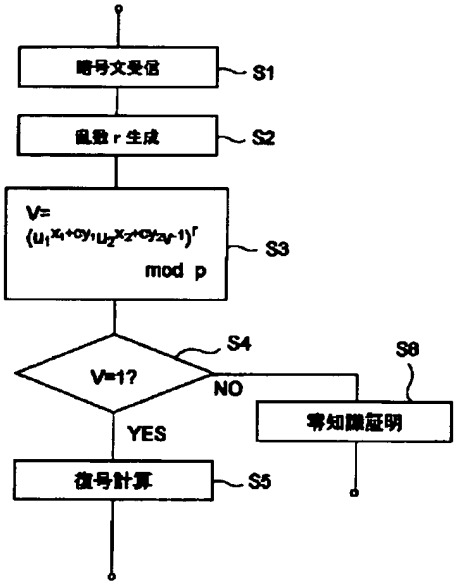

図２

S1　Cryptogram reception
S2　Random-number r generation

S5　Decoding calculation
S6　Zero knowledge proof

【特許請求の範囲】

【請求項１】
受信した暗号文が正当に作られたものであることを、検証式の値が１になることを確認することによって検証する暗号文検証方法において、
乱数ｒを生成し、本来の検証式

[CLAIMS]

[CLAIM 1]
A cryptogram verification method, in which in the cryptogram verification method which it verifies by checking that the cryptogram which received is made justly, and that the value of a verification type is set to 1, it forms a random number r, it verifies a cryptogram by checking

の値Ｖをｒ乗した値が１になるか否かを確認することによって暗号文を検証することを特徴とする暗号文検証方法。

whether the value which squared the value V of an original verification type r is set to 1.

【請求項２】

ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐ*の位数ｑの部分群を表すものとし、ｇ１，ｇ２は、ｇ１を底とするｇ２の離散対数が未知であるＧｑの元とし、Ｈを汎用ハッシュ関数とし、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Ｚｑ^{5}を秘密鍵、Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z}mod ｐなる（Ｘ，Ｙ，Ｚ）を公開鍵とし、平文ｍに対する暗号文Ｅはｃを Ｈ（ｕ１，ｕ２）mod ｑとして ｕ１＝ｇ１^{r}mod ｐ，ｕ２＝ｇ２^{r}mod ｐ，ｖ＝Ｘ^{r} Ｙ^{cr}mod ｐなる三つ組み（ｕ１，ｕ２，ｖ）を含む暗号方法において、
復号者装置は、乱数ｒを生成し、ｃ＝Ｈ（ｕ１，ｕ２）mod ｑを計算し、

[CLAIM 2]

A cryptogram verification method, in which considering it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, Gq shall express the partial group of the digit q of multiplicative-group Zp^{*}.
G1 and g2 carry out g1 the origin of Gq with a discrete unknown logarithm of g2 which it uses as a bottom, let H be a general purpose hash function, it is a secret key about (x1,x2,y1,y2,z)(element of)Zq^{5}, $x=g1^{x1}g2^{x2}$mod p, $y=g1^{y1}g2^{y2}$mod p
Let $Z=g1^{z}$ mod p be public key (X, Y, Z), the cryptogram E with respect to Plaintext m
C, as H(u1,u2)mod q
Becomes $u1=g1^{r}$mod p, $u2=g2^{r}$mod p, and $v=X^{r}Y^{cr}$mod p.
In the cryptographic method containing 3 sets (u1, u2, v), a decoding person apparatus forms a random number r, it calculates c=H(u1, u2) mod q,

Ｖ＝（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐを計算し、Ｖが１に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

V= (calculating $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p)
It verifies the correctness of a cryptogram, when V checks that it is equal to 1.

【請求項３】

請求項２の暗号文検証方法に

[CLAIM 3]

In the cryptogram verification method of Claim

おいて、Ｖが１に等しくない場合に、
零知識証明を用いて第三者にＶがある乱数ｒに対して（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐのように計算した結果であることを証明することを特徴とする暗号文検証方法。

2, when V is not equal to 1, to the random number r which has V to a third person using zero knowledge proof (it proves that it is the result of calculating like $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p.)
The cryptogram verification method characterized by the above-mentioned.

【請求項４】
ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｑの部分群を表すものとし、ｇ１，ｇ２をＧｑの元とし、Ｈを汎用ハッシュ関数とし、
ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊは固有の公開値ｗｊを持ち、
（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Ｚｑ^{5}を３ｔ＜ｎを満たすしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）を復号者Ｐｊの秘密鍵とし、
Ｘｊ＝ｇ１^{x1j} ｇ２^{x2j} mod ｐ，
Ｙｊ＝ｇ１^{y1j} ｇ２^{y2j} mod ｐ，
Ｚｊ＝ｇ１^{zj}mod ｐなる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とし、

[CLAIM 4]
A cryptogram verification method, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative group Zp.
It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, it sets n persons' decoding person to P1-Pn, each decoding person Pj has the inherent open value wj, (x1,x2,y1,y2,z)
Let the secret value (x1 j, x2 j, y1 j, y2 j, zj) corresponding to a value wj acquired by dispersing (element of)Zq^{5} with the secret dispersion method of threshold-value t which fills 3 t<n be the decoding person's Pj secret key, let $Xj=g1^{x1j}g2^{x2j}$ mod p, $Yj=g1^{y1j}g2^{y2j}$ mod p, and $Zj=g1^{zj}$mod p be the decoding person's Pj public key (Xj, Yj, Zj),

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信す

A safe communication channel shall be between each decoding person apparatus.
Moreover, that each decoding person apparatus receives the content with all the members' same

ることが保証される放送型通信路を利用できるものとし、
乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値ｒｊを復号者Ｐｊは保持するものとし、
Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を、$X=g1^{x1}g2^{x2} \bmod p$，$Y=g1^{y1}g2^{y2} \bmod p$，$Z=g1^{z} \bmod p$を公開鍵とした平文ｍの暗号文とし、正しい暗号文は$u1=g1^{r} \bmod p$，$u2=g2^{r} \bmod p$，ｃ＝Ｈ（ｕ１，ｕ２），$v=X^{r}Y^{cr} \bmod p$，$e=mZ^{r} \bmod p$を満足するとき、
Ｅを受信した各復号者Ｐｊの装置は、ｃ＝Ｈ（ｕ１，ｕ２）を計算し、

other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.
The decoding person Pj shall maintain the secret value rj corresponding to a value wj acquired by dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t.
Let E= (u1, u2, v, e) be the cryptogram of plaintext m which used $X=g1^{x1}g2^{x2} \bmod p$, $Y=g1^{y1}g2^{y2} \bmod p$, and $Z=g1^{z} \bmod p$ as public key, when the correct cryptogram satisfies $u1=g1^{r} \bmod p$, $u2=g2^{r} \bmod p$, c=H (u1, u2), $v=X^{r}Y^{cr} \bmod p$, and $e=mZ^{r} \bmod p$, the apparatus of each decoding person Pj who received E calculates c=H (u1, u2),

Ｖｊ＝（$u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1})^{rj} \bmod p$を計算し、
Ｖｊをしきい値ｔ以上２ｔ以下の検証可能秘密分散法により分散して得られる、値ｗｋに対応する秘密値Ｖｊｋを各復号者Ｐｋの装置に安全な通信路を介して送信し、
他の全ての復号者装置からＶｊｋを受信した復号者Ｐｋの装置は、放送型通信路により、Ｖｋを他の全ての復号者装置へ送信し、
Ｖｋを受信した各復号者Ｐｊの装置は対応するＶｋｊを放送型通信路により他の全ての復号者

Vj= (calculating $u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1})^{rj} \bmod p$)
It transmits the secret value Vjk corresponding to a value wk acquired by dispersing Vj with t or more threshold values and a verifiable secret dispersion method 2t or less through a communication channel safe for each decoding person's Pk apparatus, the apparatus of the decoding person Pk who received Vjk from all other decoding person apparatus transmits Vk to all other decoding person apparatus according to a broadcast type communication channel, the apparatus of each decoding person Pj who received Vk transmits corresponding Vkj to all other decoding person apparatus according to a broadcast type communication channel, it verifies that each

装置へ送信し、各復号者装置は各Ｖｋが正しい値であることを受信した全てのＶｋｊを用いて検証し、

decoding person apparatus is each value with correct Vk using all Vkj(s) that received,

正しいと確認されたＶｋのうち２ｔ＋１個を選択し、指数部に対する秘密復元手順により復元した値Ｖが１に等しいか否かを調べ、等しくないならば他の２ｔ＋１個の組み合わせで同様に秘密復元手順を繰り返し、全ての組み合わせについていずれも復元値が１に等しくないならば、その暗号文を不正と判定し、一つでも１になる組み合わせがあったならば、その暗号文を正しいと判定することを特徴とする暗号文検証方法。

If correct, it will choose 2t+1 piece among checked Vk(s), it examines whether the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1, if not equal, it repeats a secret decompression procedure similarly in other 2t+1 piece combination, about all combination, if the decompression value is not all equal to 1, it will judge that the cryptogram is irregular, if there is combination set to 1 at least one, it will judge that the cryptogram is correct.

【請求項５】
請求項４の暗号文検証方法において、
上記暗号文が正しいと判定されると、
ｗを mod ｑでの１のｎ乗根とし、各復号者装置は、ｗｊをｗ$^{j-1}$ mod ｑとし、１＜ｊ＜ｎにおいてｗｊ≠１を満たすようなｗｊを公開の固有値とし、
各復号者Ｐｊの装置はＤｊ＝ｕ１^{zj}mod ｐを計算し、放送型通信路により他の全ての復号者装置へ送信し、受信した（Ｄ１，…，Ｄｎ）のｕ１を底とする離散対数がＢＣＨ符号のコードワ

[CLAIM 5]
A cryptogram verification method, in which in the cryptogram verification method of Claim 4, if judged with the above-mentioned cryptogram being correct, let w be n root of 1 in mod q, each decoding person apparatus makes wj w^{j-1} mod q, it considers it as the eigenvalue of public presentation of wj which fills wj!=1 in 1<j<n, each decoding person's Pj apparatus calculates Dj=u1^{zj}mod p, it transmits to all other decoding person apparatus according to a broadcast type communication channel, it checks that the discrete logarithm which uses as a bottom u1 which received (D1..., Dn) is the coding word of a BCH code.

ードであることを確認すること、を特徴とする暗号文検証方法。

【請求項６】

ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐ*の位数ｑの部分群を表すものとし、ｇ１，ｇ２は、ｇ１を底とするｇ２の離散対数が未知であるＧｑの元とし、Ｈを汎用ハッシュ関数とし、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Ｚｑ^{5}を秘密鍵、Ｘ＝ｇ１^{x1}ｇ２^{x2}ｍｏｄ ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}ｍｏｄ ｐ，Ｚ＝ｇ１^{z}ｍｏｄ ｐなる（Ｘ，Ｙ，Ｚ）を公開鍵とし、平文ｍに対する暗号文Ｅはｃを Ｈ（ｕ１，ｕ２）ｍｏｄ ｑとして ｕ１＝ｇ１^{r}ｍｏｄ ｐ，ｕ２＝ｇ２^{r}ｍｏｄ ｐ，ｖ＝Ｘ^{r} Ｙ^{cr}ｍｏｄ ｐなる三つ組み（ｕ１，ｕ２，ｖ）を含む暗号方法において、

復号者装置は、乱数ｒを生成し、ｘ１′＝ｘ１・ｒｍｏｄ ｑ，ｘ２′＝ｘ２・ｒｍｏｄ ｑ，ｙ１′＝ｙ１・ｒｍｏｄ ｑ，ｙ２′＝ｙ２・ｒｍｏｄ ｑを計算し、

受信した暗号文から、ｃ＝Ｈ（ｕ１，ｕ２）ｍｏｄ ｑを計算し、Ｖ＝ｕ１$^{x1'+cy1'}$ ｕ２$^{x2'+cy2'}$ｖ$^{-r}$ｍｏｄ ｐを計算し、Ｖが１に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

[CLAIM 6]

A cryptogram verification method, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative-group Zp^{*}.

G1 and g2 carry out g1 the origin of Gq with a discrete unknown logarithm of g2 which it uses as a bottom, let H be a general purpose hash function, (x1,x2,y1,y2,z)

Let a secret key, $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$mod p, and $Z=g1^{z}$ mod p be public key for (element of)Zq^{5} (X, Y, Z), the cryptogram E with respect to Plaintext m

Making c into H(u1,u2)mod q.

U1=$g1^{r}$ mod p, u2=$g2^{r}$ mod p, it becomes $v=X^{r}$ Y^{cr}mod p.

In the cryptographic method containing 3 sets (u1, u2, v), a decoding person apparatus forms a random number r, it calculates x1'=x1 and rmod q, x2'-x2 and rmod q, y1'=y1 and rmod q, and y2'-y2 and rmod q,

From the cryptogram which received, it calculates c=H(u1, u2) mod q, it calculates $V=u1^{x1'+cy1'}$ $u2^{x2'+cy2'}v^{-r}$mod p, it verifies the correctness of a cryptogram, when V checks that it is equal to 1.

【請求項７】
請求項６の暗号文検証方法において、
Ｖが１に等しくない場合に、復号者装置は（Ｘ，Ｙ，Ｖ）が、ある（ｘ１，ｘ２，ｙ１，ｙ２，ｒ）に対してＸ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｖ＝ｕ１$^{x1r+cy1r}$ ｕ２$^{x2r+cy2r}$ ｖ$^{-r}$mod ｐを満足することを零知識証明を用いて（ｘ１，ｘ２，ｙ１，ｙ２）を秘密としたまま検証者に証明することを特徴とする暗号文検証方法。

[CLAIM 7]
A cryptogram verification method, in which in the cryptogram verification method of Claim 6, when V is not equal to 1, as for a decoding person apparatus, (X, Y, V), receive that it is (x1, x2, y1, y2, r).
It zero-knowledge-proves satisfying $X=g1^{x1}g2^{x2}$mod-p,$Y=g1^{y1}g2^{y2}$mod-p,$V=u1^{x1r+cy1r}$ $u2^{x2r+cy2r}$ v^{-r}mod p.
Using this, it proves to a verification person, making secret (x1, x2, y1, y2).

【請求項８】
請求項７の暗号文検証方法において、
ｇ，ｈはｇを底とするｈの離散対数が未知であるようなＧｑの元であって、
復号者装置は、乱数ｒ，ａ１，ａ２，ｂ１，ｂ２を生成し、
Ｒ＝ｇ^{r}ｈ^{a}mod ｐ、ＲＸ１＝Ｒ^{x1}ｈ^{a1}mod ｐ、ＲＸ２＝Ｒ^{x2}ｈ^{a2}mod ｐ、ＲＹ１＝Ｒ^{y1}ｈ^{b1}mod ｐ、ＲＹ２＝Ｒ^{y2}ｈ^{b2}mod ｐなるＲ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を公開し、

[CLAIM 8]
A cryptogram verification method, in which in the cryptogram verification method of Claim 7, g and h are under Gq whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that a decoding person apparatus forms random numbers r, a1, a2, b1, and b2, it exhibits R,RX1,RX2,RY1,RY2 used as $R=g^{r}$ h^{a} mod p,$RX1=R^{x1}h^{a1}$mod-p,$RX2=R^{x2}h^{a2}$mod-p,$RY1=R^{y1}h^{b1}$mod-p,$RY2=R^{y2}h^{b2}$mod p,

（Ｘ，Ｙ，Ｖ，Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２）がある（ｘ１，ｘ２，ｙ１，ｙ２，ｒ，ａ，ａ１，ａ２，ｂ１，ｂ２）に対して、Ｘ＝ｇ１^{x1}ｇ２^{x2}mod

To (x1,x2,y1,y2,r,a,a1,a2,b1,b2) with (X,Y,V,R,RX1,RX2,RY1,RY2), $x=g1^{x1}g2^{x2}$mod p, $y=g1^{y1}g2^{y2}$mod p, $v=u1^{x1r+cy1r}$ $u2^{x2r+cy2r}$ v^{-r}mod p, $r=g^{r}$ h^{a} mod p, $RX1=R^{x1}h^{a1}$mod p, $RX2=R^{x2}h^{a2}$mod p, $RY1=R^{y1}h^{b1}$mod p,

p，Y＝g 1 ^{y1} g 2 ^{y2}mod p，V ＝ u 1 $^{x1r+cy1r}$ u 2 $^{x2r+cy2r}$ v $^{-r}$mod p，R ＝ g ^{r} h ^{a} mod p，RX1＝R^{x1}h^{a1}mod p、RX2＝R^{x2}h^{a2}mod p、RY1＝R^{y1}h^{b1}mod p、RY2＝R^{y2}h^{b2}mod pなる関係式を満たすことを零知識証明によって証明することを特徴とする暗号文検証方法。

RY2=R^{y2}h^{b2}mod p
It proves filling the relation used as this by zero knowledge proof.

【請求項９】
請求項６の暗号文検証方法において、
ｎ人の復号者をＰ１～Ｐｎとし、
ｗを mod ｑでの１のｎ乗根とし、ｗｊをw^{j-1} mod ｑとし、１＜ｊ＜ｎにおいてｗｊ≠１を満たすものとし、各復号者Ｐｊに値ｗｊを割り当て、
復号者Ｐｊの秘密鍵（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）は、３ｔ＜ｎを満たすしきい値ｔの秘密分散法により（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）を分散して得られる、値ｗｊに対応する秘密値とし、

[CLAIM 9]
A cryptogram verification method, in which in the cryptogram verification method of Claim 6, it sets n persons' decoding person to P1-Pn, let w be n root of 1 in mod q, it makes wj into w^{j-1} mod q, in 1<j<n, it shall fill wj!=1.
It assigns each decoding person Pj a value wj, let the decoding person's Pj secret key (x1 j, x2 j, y1 j, y2 j, zj) be the secret value corresponding to a value wj acquired by dispersing (x1, x2, y1, y2, z) with the secret dispersion method of threshold-value t which satisfies 3 t<n,

Ｘｊ＝ｇ１^{x1j} ｇ２^{x2j} mod ｐ，Ｙｊ＝ｇ１^{y1j} ｇ２^{y2j} mod ｐ，Ｚｊ＝ｇ１^{Zj}mod ｐなる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とし、
各々の復号者装置間には、安全な通信路があるものとし、また、

Let Xj=g1^{x1j} g2^{x2j} mod p, Yj=g1^{y1j} g2^{y2j} mod p, and Zj=g1^{Zj}mod p be the decoding person's Pj public key (Xj, Yj, Zj), a safe communication channel shall be between each decoding person apparatus.
Moreover, that each decoding person apparatus receives the content with all the members' same

各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、
乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値ｒｊを復号者Ｐｊは保持するものとし、
各復号者Ｐｊの装置は、ｒ・ｘ１，ｒ・ｘ２，ｒ・ｙ１，ｒ・ｙ２をそれぞれしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′を分散乗算法によって計算して保持し、

other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.
The decoding person Pj shall maintain the secret value rj corresponding to a value wj acquired by dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t.
Each decoding person's Pj apparatus calculates and maintains secret value x1j' corresponding to a value wj obtained by each dispersing r-x1, r-x2, r-y1, and r-y2 with the secret dispersion method of threshold-value t, x2j', y1j', and y2j' by the distributed multiplying method,

暗号文を受信した各復号者Ｐｊの装置は、ｃ＝Ｈ（ｕ１，ｕ２）を計算し、$Vj=u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$を計算し、放送型通信路により、Ｖｊを他の全ての復号者装置へ送信し、（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認し、
指数部に対する秘密復元手順により復元した値Ｖが１に等しいことを確認することによって暗号文の正当性を検証することを特徴とする暗号文検証方法。

The apparatus of each decoding person Pj who received the cryptogram calculates c=H (u1, u2), it calculates $Vj=u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$, according to a broadcast type communication channel, it transmits Vj to all other decoding person apparatus, it checks that the index part of (V1..., Vn) is the coding word of a BCH code, it verifies the correctness of a cryptogram by checking that the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1.

【請求項１０】
請求項９の暗号文検証方法において、

[CLAIM 10]
A cryptogram verification method, in which in the cryptogram verification method of Claim 9, it

しきい値ｔを２ｔ＜ｎを満たすものとし、（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する代わりに、各復号者Ｐｊの装置が、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの正しい計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明し、

零知識証明が失敗した復号者Ｐｊを逸脱者として特定し、逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

shall fill 2 t<n for threshold-value t.

Instead of checking that the index part of (V1..., Vn) is the coding word of a BCH code, each decoding person's Pj apparatus

Without Vj leaks the information concerning that it is the correct calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j',x2j',y1j',y2j',rj, it proves to another decoding person apparatus by zero knowledge proof, it specifies the decoding person Pj in whom zero knowledge proof failed as a deviation person, another decoding person apparatus decompresses a deviation person's secret value x1j', x2j', y1j', y2j', and rj using a secret value recovery procedure.

【請求項１１】

請求項９の暗号文検証方法において、

（Ｖ１，…，Ｖｎ）がＢＣＨ符号のコードワードでない場合に、各復号者Ｐｊの装置は、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明し、証明に失敗した復号者Ｐｊの装置を逸脱者の装置と特定し、逸脱者の装置の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，

[CLAIM 11]

In the cryptogram verification method of Claim 9, when (V1..., Vn) are not the coding words of a BCH code, it proves each decoding person's Pj apparatus to another decoding person apparatus by zero knowledge proof, without leaking the information concerning [that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j', x2j', y1j', y2j', and rj, it specifies the apparatus of the decoding person Pj who failed in proof with a deviation person's apparatus, another decoding person apparatus decompresses secret value x1j' of a deviation person's apparatus, x2j', y1j', y2j', and rj using a secret value recovery procedure.

The cryptogram verification method

ｙ２ｊ′，ｒｊを、他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

characterized by the above-mentioned.

【請求項１２】
請求項９の暗号文検証方法において、
上記復元した値Ｖが１に等しい場合に、各復号者Ｐｊの装置はＤｊ＝ｕ１^{zj}mod ｐを計算し、放送型通信路により他の全ての復号者装置へ送信し、
受信した（Ｄ１，…，Ｄｎ）のｕ１を底とする離散対数がＢＣＨ符号のコードワードであることを確認することを特徴とする暗号文検証方法。

[CLAIM 12]
A cryptogram verification method, in which in the cryptogram verification method of Claim 9, when the above-mentioned value V which decompressed is equal to 1, each decoding person's Pj apparatus calculates Dj=u1^{zj}mod p, it transmits to all other decoding person apparatus according to a broadcast type communication channel, it checks that the discrete logarithm which uses as a bottom u1 which received (D1..., Dn) is the coding word of a BCH code.

【請求項１３】
請求項１０の暗号文検証方法において、
復元した値Ｖが１に等しい場合に、各復号者Ｐｊの装置はＤｊ＝ｕ１^{zj}mod ｐを計算し、Ｄｊが正しい計算結果であることをｚｊに関する情報を漏らすことなく、零知識証明によって他の復号者に証明し、
零知識証明に失敗した復号者Ｐｊを逸脱者として特定し、逸脱者の秘密値ｚｊを他の復号者装置が秘密値回復手順を用いて復元することを特徴とする暗号文検証方法。

[CLAIM 13]
A cryptogram verification method, in which in the cryptogram verification method of Claim 10, in each decoding person's Pj apparatus, the decompressed value V calculates Dj=u1^{zj}mod p, when equal to 1, dj is the correct calculation result.
Without it leaks the information about zj, it proves to another decoding person by zero knowledge proof, it specifies the decoding person Pj who failed in zero knowledge proof as a deviation person, another decoding person apparatus decompresses a deviation person's secret value zj using a secret value recovery procedure.

【請求項１４】
請求項１２又は１３の暗号文検証方法において、
各復号者装置は正しい（Ｄ１，…，Ｄｎ）から、
ｕ１を底とする指数部に対する秘密復元手順によりＤ＝ｕ１^{z} mod ｐを復元し、
ｍ＝ｅ／Ｄmod ｐを計算して平文ｍを復号することを特徴とする暗号文検証方法。

[CLAIM 14]
A cryptogram verification method, in which in the cryptogram verification method of Claim 12 or 13, from it being correct (D1..., Dn), each decoding person apparatus decompresses $D=u1^{z}$ mod p with the secret decompression procedure with respect to the index part which uses u1 as a bottom, calculates m=e/Dmod p, and decodes Plaintext m.

【請求項１５】
ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｐの部分群を表すものとし、ｇ１，ｇ２をＧｐの元とし、Ｈを汎用ハッシュ関数とし、$X=g1^{x1}g2^{x2}$mod ｐ，$Y=g1^{y1}g2^{y2}$mod ｐ，$Z=g1^{z}$ mod ｐを暗号化手順に用いる公開鍵とし、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Zq^{5}とし、平文ｍに対する暗号文Ｅはｃを$H(u1, u2)$ mod ｐとして$u1=g1^{r}$ mod ｐ，$u2=g2^{r}$ mod ｐ，$v=X^{r}Y^{cr}$mod ｐなる三つ組み（ｕ１，ｕ２，ｖ）を含み、
乱数ｒを生成する処理と、
暗号文Ｅを受信する処理と、
ｃ＝Ｈ（ｕ１，ｕ２）mod ｑを計算する処理と、

[CLAIM 15]
It considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit p of multiplicative group Zp.
It carries out g1 and g2 the origin of Gp, let H be a general purpose hash function, let $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$modp, and $Z=g1^{z}$ mod p be the public key which it uses for an encryption procedure, (x1, x2, y1, y2, z) It considers it as (element of)Zq^{5}, the cryptogram E with respect to Plaintext m
It is considering c as H(u1, u2) modp.
The 3 sets (u1, u2, v) used as $u1=g1^{r}$ mod p,$u2=g2^{r}$ mod p,$v=X^{r}Y^{cr}$mod p are included, processing which forms a random number r, processing which receives Cryptogram E, processing which calculates c=H(u1, u2) mod q,

$V=(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod ｐを計算する処理と、

V= (processing which calculates $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p)

Ｖ＝１であることを確認して暗号文の正当性を検証する処理とを復号者装置のコンピュータに実行させるプログラムを記録した記録媒体。

The recording medium on which was recorded the program which lets the computer of a decoding person apparatus perform processing which checks that it is V= 1 and verifies the correctness of a cryptogram.

【請求項１６】

Ｖ≠１ならば、ビットコミットメント関数（ＢＣ）を用いてＢＣ（ｒ）を公開する処理と、ＢＣ（ｒ）を構成するｒと、公開鍵Ｘ，Ｙを構成するｘ１，ｘ２，ｙ１，ｙ２を用いて、$(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod ｐなる計算を行った結果がＶであることを、ｒ，ｘ１，ｘ２，ｙ１，ｙ２に関する秘密を漏らさずに零知識証明で第三者へ証明する処理とを実行させるプログラムを含むことを特徴とする記録媒体。

[CLAIM 16]

Processing which will exhibit BC (r) using bit commitment function (BC) if it becomes V!=1, r which comprises BC(r), it uses x1, x2, y1, and y2 which comprise public key X and Y, the result of having performed calculation used as $(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p is V, the recording medium characterized by including the program which performs processing which it proves to a third person by zero knowledge proof without leaking the secret about r,x1,x2,y1,y2.

【請求項１７】

ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｑの部分群を表すものとし、ｇ１，ｇ２をＧｑの元とし、Ｈを汎用ハッシュ関数とし、ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊは固有の公開値ｗｊを持ち、$(x1, x2, y1, y2, z) \in Zq^{5}$を、３ｔ＜ｎを満たすしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値（ｘ１ｊ，ｘ２ｊ，

[CLAIM 17]

It considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative group Zp.

It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, it sets n persons' decoding person to P1-Pn, let the secret value (x1 j, x2 j, y1 j, y2 j, zj) corresponding to a value wj which each decoding person Pj has the inherent open value wj, and is acquired by dispersing (element of)(x1, x2, y1, y2, z) Zq^{5} with the secret

ｙ１ｊ，ｙ２ｊ，ｚｊ）を復号者Ｐｊの秘密鍵とし、Ｘｊ＝ｇ１^{x1j}ｇ２^{x2j} mod ｐ，Ｙｊ＝ｇ１^{y1j}ｇ２^{y2j} mod ｐ，Ｚｊ＝ｇ１^{zj}mod ｐを復号者Ｐｊの公開鍵とし、
乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散して得られる値ｗｊに対応する秘密値ｒｊを生成する処理と、
Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z} mod ｐを公開鍵とし、平文ｍの暗号文とし、正しい暗号文はｕ１＝ｇ１^{r}mod ｐ，ｕ２＝ｇ２^{r} mod ｐ，ｃ＝Ｈ（ｕ１，ｕ２），ｖ＝Ｘ^{r}Ｙ^{cr}mod ｐ，ｅ＝ｍＺ^{r} mod ｐを満たして暗号文Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を受信する処理と、
ｃ＝Ｈ（ｕ１，ｕ２）を計算する処理と、

dispersion method of threshold-value t which fills 3 t<n be the decoding person's Pj secret key, let Xj=g1^{x1j}g2^{x2j}mod p, Yj=g1^{y1j}g2^{y2j}mod p, and Zj=g1^{zj}mod p be the decoding person's Pj public key, processing which forms the secret value rj corresponding to the value wj obtained by dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t, let X=g1^{x1}g2^{x2}mod p, Y=g1^{y1}g2^{y2}mod p, and Z=g1^{z} mod p be public key, it considers it as the cryptogram of Plaintext m, the correct cryptogram is processing which fills u1=g1^{r} mod p, u2=g2^{r} mod p, c=H (u1, u2), v=X^{r}Y^{cr}mod p, and e=mZ^{r} mod p, and receives cryptogram E= (u1, u2, v, e), processing which calculates c=H (u1, u2),

Ｖｊ＝（ｕ１$^{x1j+cy1j}$ｕ２$^{x2j+cy2j}$ｖ$^{-1}$）^{rj}mod ｐを計算する処理と、
Ｖｊをしきい値ｔ以上２ｔ以下の検証可能秘密分散法により分散して得られる、値ｗｋに対応する秘密値Ｖｊｋを各復号者Ｐｋの装置に送信する処理と、
他の全ての復号者装置Ｐｋから Ｖｋｊを受信する処理と、
Ｖｊを他の全ての復号者装置へ送信する処理と、

Vj= (processing which calculates u1$^{x1j+cy1j}$u2$^{x2j+cy2j}$v^{-1})^{rj}mod p)
Processing which transmits the secret value Vjk corresponding to a value wk acquired by dispersing Vj with t or more threshold values and a verifiable secret dispersion method 2t or less to each decoding person's Pk apparatus, processing which receives Vkj from all other decoding person apparatus Pk, processing which transmits Vj to all other decoding person apparatus,

他の全ての復号者装置からＶｋ

Processing which receives Vk from all other

を受信する処理と、
Ｖｋｊを他の全ての復号者装置へ送信する処理と、
各Ｖｋが正しい値であることを他の全ての復号者装置からのＶｋｊを用いて検証する処理と、
正しいと確認されたＶｋのうち２ｔ＋１個を選択し、指数部に対する秘密復元手順により復元した値Ｖが１に等しいか否かを調べ、等しくないならば他の２ｔ＋１個の組み合わせで同様に秘密復元手順を繰り返し、全ての組み合わせについていずれも復元値が１に等しくないなら、その暗号文を不正と判定し、一つでも１になる組み合わせがあったならば、その暗号文を正しいと判定する処理と、を復号者装置のコンピュータに実行させるプログラムを記録した記録媒体。

decoding person apparatus, processing which transmits Vkj to all other decoding person apparatus, processing which verifies that each Vk is the correct value using Vkj from all other decoding person apparatus, if correct, it will choose 2t+1 piece among checked Vk(s), it examines whether the value V decompressed with the secret decompression procedure with respect to an index part is equal to 1, if not equal
It repeats a secret decompression procedure similarly in other 2t+1 piece combination, about all combination, if the decompression value is not all equal to 1, it will judge that the cryptogram is irregular, the recording medium on which was recorded the program which will let the computer of a decoding person apparatus perform processing which judges that the cryptogram is correct if there is combination set to 1 at least one.

【請求項１８】
ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｑの部分群を表すものとし、ｇ１，ｇ２をＧｑの元とし、Ｈを汎用ハッシュ関数とし、
（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈$Ｚｑ^{5}$を秘密鍵、Ｘ＝$ｇ１^{x1}ｇ２^{x2}$mod ｐ，Ｙ＝$ｇ１^{y1}ｇ２^{y2}$mod ｐ，Ｚ＝$ｇ１^{z}$mod ｐなる（Ｘ，Ｙ，Ｚ）を公開鍵とし、平文ｍに対する暗号文Ｅはｃを

[CLAIM 18]
It considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative group Zp.
It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, (x1,x2,y1,y2,z)
Let a secret key, $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$mod p, and $Z=g1^{z}$ mod p be public key for (element of)Zq^{5} (X, Y, Z), the 3 sets (u1, u2, v) which the cryptogram E with respect

H（ｕ１，ｕ２）mod ｑとしてｕ１＝ｇ１^{r} mod ｐ，ｕ２＝ｇ２^{r}mod ｐ，ｖ＝Ｘ^{r} Ｙ^{cr}mod ｐなる三つ組み（ｕ１，ｕ２，ｖ）を含み、
乱数ｒを生成する処理と、

to Plaintext m makes c H(u1,u2)mod q, and constitute u1=g1^{r} mod p,u2=g2^{r} mod p,v=X^{r} Y^{cr}mod p are included, processing which forms a random number r,

上記ｒを用いてｘ１′＝ｘ１・ｒmod ｑ，ｘ２′＝ｘ２・ｒmod ｑ，ｙ１′＝ｙ１・ｒmod ｑ，ｙ２′＝ｙ２・ｒmod ｑを計算する処理と、
暗号文Ｅを受信する処理と、
受信した暗号文から、ｃ＝Ｈ（ｕ１，ｕ２）mod ｑを計算し、Ｖ＝ｕ１$^{x1'+cy1'}$ｕ２$^{x2'+cy2'}$ｖ$^{-r}$mod ｐを計算する処理と、
上記Ｖが１に等しいことを確認することによって暗号文の正当性を検証する処理とを復号者装置のコンピュータに実行させるプログラムを記録した記録媒体。

Processing which calculates x1'=x1 and rmod q, x2'-x2 and rmod q, y1'=y1 and rmod q, and y2'-y2 and rmod q using the above-mentioned r, processing which receives Cryptogram E, from the cryptogram which received, it calculates c=H(u1, u2) mod q, processing which calculates V=u1$^{x1'+cy1'}$u2$^{x2'+cy2'}$v^{-r}mod p, the recording medium on which was recorded the program which lets the computer of a decoding person apparatus perform processing which verifies the correctness of a cryptogram when the above-mentioned V checks that it is equal to 1.

【請求項１９】
請求項１８の記録媒体において、
Ｖが１に等しくない場合に、（Ｘ，Ｙ，Ｖ）が、ある（ｘ１，ｘ２，ｙ１，ｙ２，ｒ）に対してＸ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｖ＝ｕ１$^{x1r+cy1r}$ ｕ２$^{x2r+cy2r}$ｖ$^{-r}$mod ｐを満足することを零知識証明を用いて（ｘ１，ｘ２，ｙ１，ｙ２，ｒ）を秘密としたまま検証

[CLAIM 19]
In the recording medium of Claim 18, in V, to the case of not being equal to 1, (X, Y, V) are X=g1^{x1}g2^{x2}mod p for it being (x1, x2, y1, y2, r), y=g1^{y1}g2^{y2}mod p, use zero knowledge proof for satisfying V=u1$^{x1r+cy1r}$ u2$^{x2r+cy2r}$v^{-r}mod p.
Have made secret (x1, x2, y1, y2, r).
The recording medium characterized by the above-mentioned program including the program which lets the above-mentioned computer perform processing which it proves to a verification person.

者に証明する処理を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項２０】
請求項１９の記録媒体において、
ｇ，ｈはｇを底とするｈの離散対数が未知であるようなＧｑの元であって、
乱数ｒ，ａ１，ａ２，ｂ１，ｂ２を生成する処理と、
$R=g^r h^a \bmod p$、$RX1=R^{x1} h^{a1} \bmod p$、$RX2=R^{x2} h^{a2} \bmod p$、$RY1=R^{y1} h^{b1} \bmod p$、$RY2=R^{y2} h^{b2} \bmod p$なるＲ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を公開する処理と、

（Ｘ，Ｙ，Ｖ，Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２）がある（ｘ１，ｘ２，ｙ１，ｙ２，ｒ，ａ，ａ１，ａ２，ｂ１，ｂ２）に対して、
$X=g1^{x1} g2^{x2} \bmod p$，$Y=g1^{y1} g2^{y2} \bmod p$，$V=u1^{x1r+cy1r} u2^{x2r+cy2r} v^{-r} \bmod p$，$R=g^r h^a \bmod p$，$RX1=R^{x1} h^{a1} \bmod p$、$RX2=R^{x2} h^{a2} \bmod p$、$RY1=R^{y1} h^{b1} \bmod p$、$RY2=R^{y2} h^{b2} \bmod p$なる関係式を満たすことを零知識証明によって証明する処理とを上記コンピュータ

[CLAIM 20]
In the recording medium of Claim 19, g and h are under Gq whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that processing which forms random numbers r, a1, a2, b1, and b2, processing which exhibits R, RX1, RX2, RY1, and RY2 used as $R=g^r h^a \bmod p$,$RX1=R^{x1}h^{a1} \bmod p$,$RX2=R^{x2}h^{a2} \bmod p$,$RY1=R^{y1}h^{b1} \bmod p$,$RY2=R^{y2}h^{b2} \bmod p$,

To (x1,x2,y1,y2,r,a,a1,a2,b1,b2) with (X,Y,V,R,RX1,RX2,RY1,RY2), $x=g1^{x1}g2^{x2} \bmod p$, $y=g1^{y1}g2^{y2} \bmod p$, $v=u1^{x1r+cy1r} u2^{x2r+cy2r} v^{-r} \bmod p$, $r=g^r h^a \bmod p$, $RX1=R^{x1}h^{a1} \bmod p$, $RX2=R^{x2}h^{a2} \bmod p$, $RY1=R^{y1}h^{b1} \bmod p$, the recording medium characterized by the above-mentioned program including the program which lets the above-mentioned computer perform processing which proves filling the relation used as $RY2=R^{y2}h^{b2} \bmod p$ by zero knowledge proof.

に実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項２１】
請求項１８の記録媒体において、
ｎ人の復号者をＰ１～Ｐｎとし、ｗを mod ｑでの１のｎ乗根とし、ｗｊをw^{j-1} mod ｑとし、１＜ｊ＜ｎにおいてｗｊ≠１を満たすものとし、各復号者Ｐｊに値ｗｊを割り当て、
復号者Ｐｊの秘密鍵（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）は、３ｔ＜ｎを満たすしきい値ｔの秘密分散法により（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）を分散して得られる、値ｗｊに対応する秘密値とし、
$Xj = g1^{x1j}\ g2^{x2j}$ mod ｐ，
$Yj = g1^{y1j}\ g2^{y2j}$ mod ｐ，
$Zj = g1^{zj}$ mod ｐなる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とし、

乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値ｒｊを保持する処理と、
ｒｘ１，ｒｘ２，ｒｙ１，ｒｙ２をそれぞれしきい値ｔの秘密分散法により分散して得られる、値ｗｊに対応する秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′を分散乗算法によって

[CLAIM 21]
In the recording medium of Claim 18, it sets n persons' decoding person to P1-Pn, let w be n root of 1 in mod q, it makes wj into w^{j-1} mod q, in 1<j<n, it shall fill wj!=1.
It assigns each decoding person Pj a value wj, let the decoding person's Pj secret key (x1 j, x2 j, y1 j, y2 j, zj) be the secret value corresponding to a value wj acquired by dispersing (x1, x2, y1, y2, z) with the secret dispersion method of threshold-value t which fills 3 t<n, let $Xj=g1^{x1j}\ g2^{x2j}$ mod p, $Yj=g1^{y1j}\ g2^{y2j}$ mod p, and $Zj=g1^{zj}$ mod p be the decoding person's Pj public key (Xj, Yj, Zj),

Processing holding the secret value rj corresponding to a value wj acquired by dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t, processing which calculates and maintains secret value x1j',x2j',y1j',y2j' corresponding to a value wj obtained by each dispersing rx1,rx2,ry1,ry2 with the secret dispersion method of threshold-value t by the distributed multiplying method, reception of a cryptogram

計算して保持する処理と、
暗号文を受信すると、ｃ＝Ｈ（ｕ１，ｕ２）を計算し、Ｖｊ＝ｕ１$^{x1j'+cy1j'}$ｕ２$^{x2j'+cy2j'}$ｖ$^{-rj}$ ｍｏｄ ｐを計算し、放送型通信路により、Ｖｊを他の全ての復号者装置へ送信する処理と、
（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する処理と、

will calculate c=H (u1, u2), it calculates Vj=u1$^{x1j'+cy1j'}$u2$^{x2j'+cy2j'}$v^{-rj} mod p, processing which transmits Vj to all other decoding person apparatus according to a broadcast type communication channel, processing which checks that the index part of (V1..., Vn) is the coding word of a BCH code,

上記指数部に対する秘密復元手順により復元した値Ｖが１に等しいことを確認することによって暗号文の正当性を検証する処理とを上記コンピュータにより実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

The recording medium characterized by the above-mentioned program including the program which performs processing which verifies the correctness of a cryptogram by checking that the value V decompressed with the secret decompression procedure with respect to the above-mentioned index part is equal to 1 by above-mentioned computer.

【請求項２２】
請求項２１の記録媒体において、
しきい値ｔを２ｔ＜ｎを満たすものとし、
（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する処理の代わりに、Ｖｊがｕ１$^{x1j'+cy1j'}$ｕ２$^{x2j'+cy2j'}$ｖ$^{-rj}$ ｍｏｄ ｐの正しい計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者に証明する処理と、
零知識証明が失敗した復号者Ｐ

[CLAIM 22]
In the recording medium of Claim 21, it shall fill 2 t<n for threshold-value t.
Instead of the processing which checks that the index part of (V1..., Vn) is the coding word of a BCH code], without Vj leaks the information concerning that it is the correct calculation result of u1$^{x1j'+cy1j'}$u2$^{x2j'+cy2j'}$v^{-rj} mod p, and] x1j',x2j',y1j',y2j',rj, processing which it proves to another decoding person by zero knowledge proof, it specifies the decoding person Pj in whom zero knowledge proof failed as a deviation person, the recording medium characterized by including the program which lets the above-mentioned computer perform a deviation person's secret value x1j', x2j', y1j',

ｊを逸脱者として特定し、逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを秘密値回復手順を用いて復元する処理とを上記コンピュータに実行させるプログラムを上記プログラムに含むことを特徴とする記録媒体。

y2j', and processing that decompresses rj using a secret value recovery procedure in the above-mentioned program.

【請求項２３】

請求項２１の記録媒体において、

（Ｖ１，…，Ｖｎ）がＢＣＨ符号のコードワードでない場合に、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者に証明する処理と、上記証明に失敗した復号者Ｐｊを逸脱者と特定し、逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを、秘密値回復手順を用いて復元する処理とを上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

[CLAIM 23]

In the recording medium of Claim 21, when (V1..., Vn) are not the coding words of a BCH code, without it leaks the information concerning that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j',x2j',y1j',y2j',rj, it specifies the processing which it proves to another decoding person by zero knowledge proof, and the decoding person Pj who failed in the above-mentioned proof with a deviation person, the recording medium characterized by the above-mentioned program including the program which lets the above-mentioned computer perform processing which decompresses a deviation person's secret value x1j', x2j', y1j', y2j', and rj using a secret value recovery procedure.

【請求項２４】

ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｑの部分群を表すものとし、ｇ１，ｇ２をＧｑの元とし、Ｈを汎用ハッ

[CLAIM 24]

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the

シュ関数とし、
（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Ｚｑ^{5}を秘密鍵、Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z}mod ｐなる（Ｘ，Ｙ，Ｚ）を公開鍵とし、平文ｍに対する暗号文Ｅはｃを Ｈ（ｕ１，ｕ２）mod ｑとして ｕ１＝ｇ１^{r}mod ｐ，ｕ２＝ｇ２^{r}mod ｐ，ｖ＝Ｘ^{r}Ｙ^{cr}mod ｐなる三つ組み（ｕ１，ｕ２，ｖ）を含む暗号文の検証装置であって、
乱数ｒを生成する手段と、

digit q of multiplicative group Zp.
It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, (x1,x2,y1,y2,z)
Let a secret key, $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$mod p, and $Z=g1^{z}$ mod p be public key for (element of)Zq^{5} (X, Y, Z), the cryptogram E with respect to Plaintext m is considering c as H(u1, u2) mod q.
It is the verification apparatus of the cryptogram containing the 3 sets (u1, u2, v) used as $u1=g1^{r}$ mod p,$u2=g2^{r}$ mod p,$v=X^{r}Y^{cr}$mod p, comprised such that means to form a random number r,

ｃ＝Ｈ（ｕ１，ｕ２）mod ｑを計算する手段と、
Ｖ＝（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐを計算する手段と、
Ｖが１に等しいことを確認することによって暗号文の正当性を検証する手段とを備えることを特徴とする暗号文検証装置。

Means to calculate c=H(u1, u2) mod q, means to calculate $V=(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p, means to verify the correctness of a cryptogram when V checks that it is equal to 1
Are provided.

【請求項２５】
請求項２４の暗号文検証装置において、
Ｖが１に等しくない場合に、
零知識証明を用いて第三者にＶが乱数ｒに対して（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐのように計算した結果であることを証明する手段を備えることを特徴とする暗号文検証装置。

[CLAIM 25]
A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 24, when V is not equal to 1, v receives a third person at a random number r using zero knowledge proof (it has means to prove that it is the result of calculating like $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p.).

【請求項２６】

[CLAIM 26]

pを大きな素数、qをp－1を割り切る大きな素数とし、Gqは乗法群Zpの位数qの部分群を表すものとし、g1，g2をGqの元とし、Hを汎用ハッシュ関数とし、
n人の復号者をP1～Pnとし、各復号者Pjは固有の公開値wjを持ち、
（x1，x2，y1，y2，z）$\in Zq^5$を、3t＜nを満たすしきい値tの秘密分散法により分散して得られる、値wjに対応する秘密値（x1j，x2j，y1j，y2j，zj）を復号者Pjの秘密鍵とし、
$Xj = g1^{x1j} g2^{x2j} \bmod p$，
$Yj = g1^{y1j} g2^{y2j} \bmod p$，
$Zj = g1^{zj} \bmod p$なる（Xj，Yj，Zj）を復号者Pjの公開鍵とし、

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative group Zp.
It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, it sets n persons' decoding person to P1-Pn, each decoding person Pj has the inherent open value wj, let the secret value (x1 j, x2 j, y1 j, y2 j, zj) corresponding to a value wj acquired by dispersing (x1,x2,y1,y2,z)(element of)Zq^5 with the secret dispersion method of threshold-value t which fills 3 t<n be the decoding person's Pj secret key, let $Xj=g1^{x1j}g2^{x2j} \bmod p$, $Yj=g1^{y1j}g2^{y2j} \bmod p$, and $Zj=g1^{zj} \bmod p$ be the decoding person's Pj public key (Xj, Yj, Zj),

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、
乱数r$\in$Zqをしきい値tの秘密分散法により分散して得られる、値wjに対応する秘密値rjを復号者Pjは保持するものとし、
E＝（u1，u2，v，e）を、$X = g1^{x1} g2^{x2} \bmod p$，$Y = g1^{y1} g2^{y2} \bmod p$，$Z = g1^{z}$

A safe communication channel shall be between each decoding person apparatus.
Moreover, that each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.
The decoding person Pj shall maintain the secret value rj corresponding to a value wj acquired by dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t.
Let E= (u1, u2, v, e) be a cryptogram with respect to plaintext m which used

mod ｐを公開鍵とした平文ｍに対する暗号文とし、正しい暗号文はｕ１＝ｇ１^{r} mod ｐ，ｕ２＝ｇ２^{r} mod ｐ，ｃ＝Ｈ（ｕ１，ｕ２），ｖ＝Ｘ^{r} Ｙ^{cr}mod ｐ，ｅ＝ｍＺ^{r} mod ｐを満足する暗号文の検証装置であって、
Ｅを受信してｃ＝Ｈ（ｕ１，ｕ２）を計算する手段と、

X=g1^{x1}g2^{x2}mod p, Y=g1^{y1}g2^{y2}mod p, and Z=g1^{z} mod p as public key, the correct cryptogram is the verification apparatus of the cryptogram which satisfies u1=g1^{r} mod p, u2=g2^{r} mod p, c=H (u1, u2), v=X^{r} Y^{cr}mod p, and e=mZ^{r} mod p, comprised such that means to calculate c=H (u1, u2) by receiving E,

Ｖｊ＝（ｕ１$^{x1j+cy1j}$ｕ２$^{x2j+cy2j}$ｖ$^{-1}$）^{rj}mod ｐを計算する手段と、
Ｖｊをしきい値ｔ以上２ｔ以下の検証可能秘密分散法により分散して、値ｗｋに対応する秘密値Ｖｊｋを得る手段と、
Ｖｊｋを各復号者Ｐｋの装置に安全な通信路を介して送信する手段と、
他の全ての復号者装置Ｐｋから Ｖｋｊを受信すると、放送型通信路により、Ｖｊを他の全ての復号者装置へ送信する手段と、

Vj= (means to calculate u1$^{x1j+cy1j}$u2$^{x2j+cy2j}$v^{-1})^{rj}mod p)
It disperses Vj with t or more threshold values and a verifiable secret dispersion method 2t or less, means to acquire the secret value Vjk corresponding to a value wk, means to transmit Vjk through a communication channel safe for each decoding person's Pk apparatus, means to transmit Vj to all other decoding person apparatus according to a broadcast type communication channel if Vkj is received from all other decoding person apparatus Pk,

Ｖｋを受信すると、対応するＶｋｊを放送型通信路により他の全ての復号者装置へ送信する手段と、
各Ｖｋが正しい値であることをＶｋｊを用いて検証する手段と、
正しいと確認されたＶｋのうち２ｔ＋１個を選択し、指数部に対する秘密復元手順によりＶを復元する手段と、
復元した値Ｖが１に等しいか否

Means to transmit corresponding Vkj to all other decoding person apparatus according to a broadcast type communication channel if Vk is received, means by which each Vk verifies using Vkj that it is the correct value, if correct, it will choose 2t+1 piece among checked Vk(s), means to decompress V with the secret decompression procedure with respect to an index part, means to examine whether the decompressed value V is equal to 1,

かを調べる手段と、

Ｖが１に等しくないならば他の２ｔ＋１個の組み合わせで同様に秘密復元手順を繰り返し、Ｖが１に等しいか否か調べる手段と、
２ｔ＋１個の全ての組み合わせについていずれも復元値が１に等しくないならば、その暗号文を不正と判定し、一つでも１になる組み合わせがあったならば、その暗号文を正しいと判定する手段と、を備えることを特徴とする暗号文検証装置。

If V is not equal to 1
It repeats a secret decompression procedure similarly in other 2t+1 piece combination, means to examine whether V is equal to 1, about all 2t+1 piece combination, if the decompression value is not all equal to 1, it will judge that the cryptogram is irregular, means to judge that the cryptogram is correct if there is combination set to 1 at least one
Are provided.

【請求項２７】
請求項２６の暗号文検証装置において、
ｗを mod ｑでの１のｎ乗根とし、各復号者は、ｗｊをw^{j-1} mod ｑとし、１＜ｊ＜ｎにおいてｗｊ≠１を満たすようなｗｊを公開の固有値とし、
Ｄｊ＝ｕ１^{zj}mod ｐを計算する手段と、
Ｄｊを放送型通信路により他の全ての復号者装置へ送信する手段と、

[CLAIM 27]
A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 26, let w be n root of 1 in mod q, each decoding person makes wj w^{j-1} mod q, it considers it as the eigenvalue of public presentation of wj which fills wj!=1 in 1<j<n, means to calculate Dj=u1^{zj}mod p, means to transmit Dj to all other decoding person apparatus according to a broadcast type communication channel,

受信した（Ｄ１，…，Ｄｎ）のｕ１を底とする離散対数がＢＣＨ符号のコードワードであることを確認する手段とを備えることを特徴とする暗号文検証装置。

Means to check that the discrete logarithm which uses as a bottom u1 which received (D1..., Dn) is the coding word of a BCH code
Are provided.

【請求項２８】

ｐを大きな素数、ｑをｐ－１を割り切る大きな素数とし、Ｇｑは乗法群Ｚｐの位数ｑの部分群を表すものとし、ｇ１，ｇ２をＧｑの元とし、Ｈを汎用ハッシュ関数とし、

（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）$\in Z_q^5$を秘密鍵、$X = g1^{x1} g2^{x2} \bmod p$，$Y = g1^{y1} g2^{y2} \bmod p$，$Z = g1^{z} \bmod p$なる（Ｘ，Ｙ，Ｚ）を公開鍵とし、平文ｍに対する暗号文Ｅはｃを$H(u1, u2) \bmod q$として$u1 = g1^{r} \bmod p$，$u2 = g2^{r} \bmod p$，$v = X^{r} Y^{cr} \bmod p$なる三つ組み（ｕ１，ｕ２，ｖ）を含む暗号文の検証装置であって、

乱数ｒを生成する手段と、

$x1' = x1 \cdot r \bmod q$，$x2' = x2 \cdot r \bmod q$，$y1' = y1 \cdot r \bmod q$，$y2' = y2 \cdot r \bmod q$を計算する手段と、

受信した暗号文から、$c = H(u1, u2) \bmod q$を計算する手段と、この計算結果と受信暗号文から、$V = u1^{x1', +cy1'} u2^{x2'+cy2'} v^{-r} \bmod p$を計算する手段と、

Ｖが１に等しいことを確認することによって暗号文の正当性を検証する手段とを備えることを

[CLAIM 28]

A cryptogram verification apparatus, which considers it as the big prime number which gives a clear-cut solution for p to a big prime number, and gives a clear-cut solution for q to p-1, gq shall express the partial group of the digit q of multiplicative group Zp.

It carries out g1 and g2 the origin of Gq, let H be a general purpose hash function, (x1,x2,y1,y2,z).

It is a secret key about (element of)Zq^5, it is set to $X=g1^{x1}g2^{x2} \bmod p, Y=g1^{y1}g2^{y2} \bmod p, Z=g1^{z} \bmod p$.

Let (X, Y, Z) be public key, the cryptogram E with respect to Plaintext m is the verification apparatus of the cryptogram containing the 3 sets (u1, u2, v) which constitute $u1=g1^{r} \bmod p, u2=g2^{r} \bmod p, v=X^{r} Y^{cr} \bmod p$ by making c into H(u1,u2)mod q, comprised such that means to form a random number r,

Means to calculate x1'=x1 and rmod q, x2'-x2 and rmod q, y1'=y1 and rmod q, and y2'-y2 and rmod q, means to calculate c=H(u1, u2) mod q from the cryptogram which received, this calculation result and means to calculate $V=u1^{x1,+cy1'} u2^{x2'+cy2'} v^{-r} \bmod p$ from a receiving cryptogram, means to verify the correctness of a cryptogram when V checks that it is equal to 1 Are provided.

特徴とする暗号文検証装置。

【請求項２９】
請求項２８の暗号文検証装置において、
Ｖが１に等しくない場合に、（Ｘ，Ｙ，Ｖ）が、ある（ｘ１，ｘ２，ｙ１，ｙ２，ｒ）に対してＸ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｖ＝ｕ１$^{x1r+cy1r}$ ｕ２$^{x2r+cy2r}$ ｖ$^{-r}$mod ｐを満足することを零知識証明を用いて（ｘ１，ｘ２，ｙ１，ｙ２，ｒ）を秘密としたまま検証者装置に証明する手段を備えることを特徴とする暗号文検証装置。

[CLAIM 29]
A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 28, when V is not equal to 1, (X Y, V), with respect to a (x1, x2, y1, y2, r).
Use zero knowledge proof for satisfying $X=g1^{x1}g2^{x2}\bmod p$, $Y=g1^{y1}g2^{y2}\bmod p$, and $V=u1^{x1r+cy1r}\ u2^{x2r+cy2r}\ v^{-r}\bmod p$.
It has means to prove to a verification person apparatus making secret (x1, x2, y1, y2, r).

【請求項３０】
請求項２９の暗号文検証装置において、
ｇ，ｈはｇを底とするｈの離散対数が未知であるようなＧｑの元であって、
乱数ｒ，ａ１，ａ２，ｂ１，ｂ２を生成する手段と、
Ｒ＝ｇ^{r}ｈ^{a}mod ｐ、ＲＸ１＝Ｒ^{x1}ｈ^{a1}mod ｐ、ＲＸ２＝Ｒ^{x2}ｈ^{a2}mod ｐ、ＲＹ１＝Ｒ^{y1}ｈ^{b1}mod ｐ、ＲＹ２＝Ｒ^{y2}ｈ^{b2}mod ｐなるＲ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を公開する手段と、

[CLAIM 30]
A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 29, g and h are under Gq whose discrete logarithm of h which uses g as a bottom is unknown, comprised such that means to form random numbers r, a1, a2, b1, and b2, means to exhibit R,RX1,RX2,RY1,RY2 used as $R=g^{r}h^{a}\bmod p$,$RX1=R^{x1}h^{a1}\bmod p$,$RX2=R^{x2}h^{a2}\bmod p$,$RY1=R^{y1}h^{b1}\bmod p$,$RY2=R^{y2}h^{b2}\bmod p$,

（Ｘ，Ｙ，Ｖ，Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２）がある

To (x1,x2,y1,y2,r,a,a1,a2,b1,b2) with (X,Y,V,R,RX1,RX2,RY1,RY2), $x=g1^{x1}g2^{x2}\bmod p$,

（ｘ１，ｘ２，ｙ１，ｙ２，ｒ，ａ，ａ１，ａ２，ｂ１，ｂ２）に対して、
$X=g1^{x1}g2^{x2} \bmod p$，$Y=g1^{y1}g2^{y2} \bmod p$，$V=u1^{x1r+cy1r}u2^{x2r+cy2r}v^{-r} \bmod p$，$R=g^{r}h^{a} \bmod p$，$RX1=R^{x1}h^{a1} \bmod p$、$RX2=R^{x2}h^{a2} \bmod p$、$RY1=R^{y1}h^{b1} \bmod p$、$RY2=R^{y2}h^{b2} \bmod p$なる関係式を満たすことを零知識証明によって証明する手段とを備えることを特徴とする暗号文検証装置。

$y=g1^{y1}g2^{y2} \bmod p$, $v=u1^{x1r+cy1r}u2^{x2r+cy2r}v^{-r} \bmod p$, $r=g^{r}h^{a} \bmod p$, $RX1=R^{x1}h^{a1} \bmod p$, $RX2=R^{x2}h^{a2} \bmod p$, $RY1=R^{y1}h^{b1} \bmod p$, $RY2=R^{y2}h^{b2} \bmod p$
Means to prove filling the relation used as this by zero knowledge proof
Are provided.

【請求項３１】
請求項２８の暗号文検証装置において、
ｎ人の復号者をＰ１～Ｐｎとし、
ｗを mod ｑでの１のｎ乗根とし、ｗｊを$w^{j-1} \bmod q$とし、１＜ｊ＜ｎにおいてｗｊ≠１を満たすものとし、各復号者Ｐｊに値ｗｊを割り当て、
（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）$\in Zq^{5}$を秘密鍵とし、$X=g1^{x1}g2^{x2} \bmod p$，$Y=g1^{y1}g2^{y2} \bmod p$，$Z=g1^{z} \bmod p$を公開鍵とし、

[CLAIM 31]
A cryptogram verification apparatus, in which in the cryptogram verification apparatus of Claim 28, it sets n persons' decoding person to P1-Pn, let w be n root of 1 in mod q, it makes wj into $w^{j-1} \bmod q$, in 1<j<n, it shall fill wj!=1.
It assigns each decoding person Pj a value wj, (x1,x2,y1,y2,z)
Let (element of)Zq^{5} be a secret key, let $X=g1^{x1}g2^{x2} \bmod p$, $Y=g1^{y1}g2^{y2} \bmod p$, and $Z=g1^{z} \bmod p$ be public key,

復号者Ｐｊの秘密鍵（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）は、３ｔ＜ｎを満たすしきい値ｔの秘密分散法により（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）を分散

Let the decoding person's Pj secret key (x1 j, x2 j, y1 j, y2 j, zj) be the secret value corresponding to a value wj acquired by dispersing (x1, x2, y1, y2, z) with the secret dispersion method of threshold-value t which fills 3 t<n, let $Xj=g1^{x1j}$

して得られる、値ｗｊに対応する秘密値とし、
Ｘｊ＝ｇ１^{x1j} ｇ２^{x2j} mod ｐ，
Ｙｊ＝ｇ１^{y1j} ｇ２^{y2j} mod ｐ，
Ｚｊ＝ｇ１^{Zj}mod ｐなる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とし、
各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとし、
乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散して、値ｗｊに対応する秘密値ｒｊを得る手段と、

g2^{x2j} mod p, Yj=g1^{y1j} g2^{y2j} mod p, and Zj=g1^{Zj}mod p be the decoding person's Pj public key (Xj, Yj, Zj), a safe communication channel shall be between each decoding person apparatus.
Moreover, that each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.
It disperses random-number r(element of)Zq with the secret dispersion method of threshold-value t, means to acquire the secret value rj corresponding to a value wj,

ｒｘ１，ｒｘ２，ｒｙ１，ｒｙ２をそれぞれしきい値ｔの秘密分散法により分散して、値ｗｊに対応する秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′を分散乗算法によって計算して得る手段と、
受信した暗号文について、ｃ＝Ｈ（ｕ１，ｕ２）を計算する手段と、Ｖｊ＝ｕ１$^{x1j'+cy1j'}$ｕ２$^{x2j'+cy2j'}$ｖ$^{-rj}$ mod ｐを計算する手段と、
放送型通信路により、Ｖｊを他の全ての復号者装置へ送信する手段と、
（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する手段と、

It each disperses rx1, rx2, ry1, and ry2 with the secret dispersion method of threshold-value t, means which it acquires by calculating secret value x1j' corresponding to a value wj, x2j', y1j', and y2j' by the distributed multiplying method, means to calculate c=H (u1, u2) about the cryptogram which received, means to calculate Vj=u1$^{x1j'+cy1j'}$u2$^{x2j'+cy2j'}$v^{-rj} mod p, means to transmit Vj to all other decoding person apparatus according to a broadcast type communication channel, means to check that the index part of (V1..., Vn) is the coding word of a BCH code,

指数部に対する秘密復元手順によりＶを復元する手段と、
復元した値Ｖが１に等しいことを確認することによって暗号文の正当性を検証する手段と、を備えることを特徴とする暗号文検証装置。

Means to decompress V with the secret decompression procedure with respect to an index part, means to verify the correctness of a cryptogram by checking that the decompressed value V is equal to 1
Are provided.

【請求項３２】
請求項３１の暗号文検証装置において、
しきい値ｔを、２ｔ＜ｎを満たすものとし、
（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する代わりに、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの正しい計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者に対し証明する手段を備えることを特徴とする暗号文検証装置。

[CLAIM 32]
In the cryptogram verification apparatus of Claim 31, it shall fill 2 t<n for threshold-value t.
It has means to prove to another decoding person by zero knowledge proof, without Vj leaking the information concerning [that it is the correct calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j', x2j', y1j', y2j', and rj instead of checking that the index part of (V1..., Vn) is the coding word of a BCH code.
The cryptogram verification apparatus characterized by the above-mentioned.

【請求項３３】
請求項３１の暗号文検証装置において、
（Ｖ１，…，Ｖｎ）がＢＣＨ符号のコードワードでない場合に、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知

[CLAIM 33]
In the cryptogram verification apparatus of Claim 31, means to prove to another decoding person by zero knowledge proof without leaking the information concerning [that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j', x2j', y1j', y2j', and rj when (V1..., Vn) are not the coding words of a BCH code, it specifies the decoding person Pj who failed in the proof with a deviation person, a deviation

識証明によって他の復号者に証明する手段と、
その証明に失敗した復号者Ｐｊを逸脱者と特定し、逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを秘密値回復手順を用いて復元する手段とを備えることを特徴とする暗号文検証装置。

person's secret value x1j', x2j', y1j', y2j', means to decompress rj using a secret value recovery procedure
Are provided.
The cryptogram verification apparatus characterized by the above-mentioned.

【発明の詳細な説明】

[DETAILED DESCRIPTION OF THE INVENTION]

【０００１】

[0001]

【発明の属する技術分野】
この発明は、電気通信システムで通信を行う場合に、通信内容を秘匿し、かつ復号内容を公開した場合にも復号者の秘密鍵に関する情報が漏れることがない安全な暗号方法に関し、特に、暗号文の正当性を復号者が検証する暗号文検証方法及びそのプログラム記録媒体、に関する。

[TECHNICAL FIELD OF THE INVENTION]
This invention relates to the safe cryptographic method from which the information about a decoding person's secret key does not leak, also when the content of communication is kept secret when communicating by a telecommunication system, and the content of decoding is exhibited.
Specifically, it is related with the cryptogram verification method that a decoding person verifies the correctness of a cryptogram, and its program recording medium.

【０００２】

[0002]

【従来の技術】
選択平文攻撃に強い暗号系においては、暗号文の送信者が元の平文を知っていることを復号者が何らかの方法で検証する。Ｃ

[PRIOR ART]
In a code type strong against a choice plaintext attack, a decoding person verifies that the transmitting party of a cryptogram knows original plaintext by a certain method.

ｒａｍｅｒ－Ｓｈｏｕｐ暗号は、論文 R.Cramer and V.Shoup: “A practical public key cryptosystem provablysecure against adaptive chosen chipertext attack ”, Advances in Cryptology-CRYPTO'98, LNCS 1462, Springer-Verlag, pp.13-25, 1998 で提案された、汎用一方向性ハッシュ関数の存在および、Diffie-Hellman 判定問題の困難性という広く信じられている仮定の下で、適応的選択暗号文攻撃に強いことが証明できる公開鍵暗号方法である。Cramer-Shoup 暗号は一つの公開鍵に対応する一つの秘密鍵を持つ一人の復号者を想定した暗号方法である。

Cramer-Shoup code, paper R.Cramer and V.Shoup:"A Practical public key Cryptosystem provablysecure Against adaptive chosen It proposed by chipertext attack", Advances in Cryptology-CRYPTO'98 and LNCS 1462, Springer-Verlag, pp.13-25, and 1998, it is the public-key cryptographic method which can prove that it is strong to an adaptive choice cryptogram attack under assumption which is called a presence of a general purpose unidirectional hash function and the difficulty of a Diffie-Hellman evaluation problem, and which is believed widely.
A Cramer-Shoup code is a cryptographic method supposing the decoding person of one person with one secret key corresponding to one public key.

【０００３】
すでに一復号者の場合に適応的選択暗号文攻撃に強いことが知られている Cramer-Shoup 暗号方法では、まず、大きな素数ｐ、ｑを、ｑがｐ－１を割り切るように選び、乗法群Ｚｐの位数ｑの部分群Ｇｑの元ｇ１，ｇ２を用いて、秘密鍵を（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈$Ｚｑ^{5}$公開鍵を$Ｘ＝ｇ１^{x1}ｇ２^{x2}$mod ｐ，$Ｙ＝ｇ１^{y1}ｇ２^{y2}$mod ｐ，$Ｚ＝ｇ１^{z}$ mod ｐとする。平文ｍ∈Ｇｑに対する暗号文Ｅは（ｕ１，ｕ２，ｖ，ｅ）より成り、正しく作成された暗号文はある乱数

[0003]
With the Cramer-Shoup cryptographic method with which it is already known in the case of the 1 decoding person that it is strong to an adaptive choice cryptogram attack
First, it chooses the big prime numbers p and q so that q may give a clear-cut solution to p-1, and it uses the origin g1 and g2 of the partial group Gq of the digit q of multiplicative group Zp, it is (element of)(x1, x2, y1, y2, z) Zq^{5} public key about a secret key, $X=g1^{x1}g2^{x2}$mod p It is referred to as $Y=g1^{y1}g2^{y2}$mod p and $Z=g1^{z}$ mod p.
The cryptogram E with respect to plaintext m(element of)Gq constitutes of (u1, u2, v, e), and the cryptogram made correctly satisfies

rに対してu1＝g1^{r} mod p，u2＝g2^{r} mod p，c＝H(u1,u2)，v＝X^{r} Y^{cr}mod p，e＝mZ^{r} mod pを満足する。この暗号文を受信した復号者は、まず、c＝H（u1，u2）を計算し、暗号文が検証式 u1^{x1+cy1} u2^{x2+cy2}≡v（mod p）を満たすか否かを検証し、満たさない場合にはその暗号文の復号を拒否し、満たす場合には、m＝e／u1^{z} mod pを計算し、平文mを得る。

u1=g1^{r} mod p, u2=g2^{r} mod p, c=H (u1, u2), v=X^{r} Y^{cr}mod p, and e=mZ^{r} mod p to a certain random number r.
The decoding person who received this cryptogram calculates c=H (u1, u2) first, it verifies whether a cryptogram fills verification type u1^{x1+cy1}u2^{x2+cy2}IDENTICAL-TOv (mod p), when not filling, it refuses decoding of the cryptogram, it calculates m=e/u1^{z} modp, when filling, it obtains Plaintext m.

【０００４】
上記検証式により、復号者は、暗号文の制作者が元の平文mを知っていることを確認することができる。検証式を満たさない不正な暗号文に対しては復号を拒否するので、攻撃者は何れの有用な情報も得られない。しかしながら、この暗号文検証方法では、検証の結果復号を拒否する場合に、第三者に対して検証した暗号文が不正であったこと、すなわち、V≡u1^{x1+cy1} u2^{x2+cy2}（mod p）として、V≠v（mod p）とならないことを、Vに関する情報を何ら情報を漏らすことなく証明するのは現実的には困難である。

[0004]
By the above-mentioned verification type, a decoding person can check that the maker of a cryptogram knows original plaintext m.
To the irregular cryptogram which does not fill a verification type, it refuses decoding, therefore, as for neither of the useful information, an aggressor is obtained.
However, when refusing decoding by this cryptogram verification method as a result of verification, it is actually difficult to prove the information concerning [not becoming V!=v (mod p) and] V, without leaking information in any way as the cryptogram verified to the third person having been illegitimate (mod p), i.e., VIDENTICAL-TOu1^{x1+cy1}u2^{x2+cy2}.

【０００５】
さらに、ＥｌＧａｍａｌ暗号などでしばしば行われるように、

[0005]
Furthermore, the thing for which secret dispersion disperses a corresponding secret

一つの公開鍵に対して、対応する秘密鍵を秘密分散により複数の部分秘密鍵に分散し、複数の復号者にこれを保持させることにより、しきい値を越える人数の復号者が協力したときのみ暗号文を復号できるようにするしきい値付き復号を適用する場合、この暗号復号方法において検証式を満たさないような不正な暗号文に対して、検証式の左辺 $u1^{x1+cy1}u2^{x2+cy2}$ の計算結果Vが複数の復号者に知れてしまうため、攻撃者と結託した復号者が存在した場合に、攻撃者に情報が漏洩してしまい、選択暗号文攻撃への安全性を保つことはできない。

key to two or more partial secret keys to one public key, and it maintains this to two or more decoding persons so that it may often be performed by the ElGamal code etc., to an irregular cryptogram which does not fill a verification type in this code decoding method when the decoding person of the number which exceeds a threshold value cooperates and it applies decoding with the threshold value which enables it to decode a cryptogram, since the calculation result V of left-side $u1^{x1+cy1}u2^{x2+cy2}$ of a verification type becomes known to two or more decoding persons, when the decoding person who conspired with the aggressor exists, information is revealed to an aggressor and it cannot maintain the safety to a choice cryptogram attack.

【０００６】

しきい値付き復号方法については、例えば、論文 V.Shoup and R.Gennaro: “ Securing threshold cryptosystems against chosen ciphertext attack ” , Advances in Cryptology-EUROCRYPT '98, LNCS 1403, Springer-Verlag, pp.1-16,1998 で提案された方式は、適応的選択暗号文攻撃に強いことがランダムオラクルの存在という仮定の下で示されている。

[0006]

About the decoding method with a threshold value

For example, paper V.Shoup and R.Gennaro : "Securing threshold Cryptosystems against Chosen ciphertext attack ", Advances in Cryptology-EUROCRYPT' 98 and LNCS 1403, Springer-Verlag, and pp.1- 16 and 1998 Proposed system, it is shown under assumption called a presence of a random oracle that it is strong to an adaptive choice cryptogram attack.

【０００７】

しかしながら、ランダムオラク

[0007]

However, assumption called a random oracle is

ルという仮定は、極めて非現実的であり、ランダムオラクルを通常の衝突困難と考えられるハッシュ関数等に置き換えて使用した場合には、その安全性について何の保証も得ることができない。

very unreal.
When a random oracle is replaced and used for the hash function considered that the usual collision is difficult, it can obtain no guarantee about the safety.

【０００８】

[0008]

【発明が解決しようとする課題】
この発明の目的は、Cramer-Shoup 暗号において、検証式における値に関する情報を一切漏らすことなく、暗号文の正当性を検証でき、また検証式の値が正当でないことを示している場合に、その値が正しく作成されたものであることを、零知識証明によって第三者に証明することが、更に複数の復号者が協力して検証する場合に、復号者中に不正者がいたとしても、検証式の値が復号者にも漏洩することがない暗号文検証方法、そのプログラム記録媒体、及びその装置を提供することにある。

[PROBLEM TO BE SCLVED BY THE INVENTION]
It sets the objective of this invention to a Cramer-Shoup code, it can verify the correctness of a cryptogram, without leaking the information about the value in a verification type entirely, moreover, the thing for which the value is correctly made when it is shown that the value of a verification type is not rightful, proving for a third person by zero knowledge proof
Furthermore, when two or more decoding persons cooperate and verify, also as there having been an irregular person in a decoding person, the value of a verification type is providing the cryptogram verification method which it does not reveal to a decoding person, either, its program recording medium, and its apparatus.

【０００９】

[0009]

【課題を解決するための手段】
Cramer-Shoup 暗号における復号時の検証式の値を、復号者の誰もがその値を知り得ない乱数

[MEANS TO SOLVE THE PROBLEM]
It carries out the power of the value of the verification type at the time of decoding in a Cramer-Shoup code with the random number

によってべき乗し、そのべき乗した結果が１となるか否かを検証することによって暗号文の正当性を検証する。この乱数でべき乗するという計算を分散計算により、全計算者の協力で行うことによって、検証式を満たさない場合にも、べき乗する前の検証式の値はどの復号者にも漏洩することはない、つまり正当でない場合は、計算値が１でない値となり、その値が乱数でべき乗されているから、そのべき乗されている値を示して計算値が１でないこと、即ち正当でないことを示しても、そのべき乗前の値はかくされ、情報が漏れるおそれはない。

with which everyone of a decoding person cannot know the value, and verifies the correctness of a cryptogram by verifying whether the result of having carried out the power is set to 1.
Also when not filling a verification type by performing calculation of carrying out a power by these random numbers, by cooperation of all accountants by distributed calculation, it reveals to no decoding person, that is, the value of the verification type before carrying out a power turns into a value whose calculated value is not 1, when not rightful, the power of the value is carried out by the random numbers, therefore
Even if the value by which the power is carried out is shown and it is shown that a calculated value is not 1, i.e., are not rightful, the value in front of the power is hidden, there is no risk that information may leak.

【００１０】
ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊ（ｊ＝１，２，…，ｎ）は固有の公開値ｗｊを持つものとする。（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈$Ｚｑ^{5}$をしきい値ｔの秘密分散法により分散し、値ｗｊに対応する秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）を復号者Ｐｊの秘密鍵とする。

[0010]
It sets n persons' decoding person to P1-Pn, each decoding person Pj (j = 1, 2..., n) shall have the inherent open value wj.
(x1,x2,y1,y2,z)
It disperses (element of)Zq^{5} with the secret dispersion method of threshold-value t, let the secret value (x1 j, x2 j, y1 j, y2 j, zj) corresponding to a value wj be the decoding person's Pj secret key.

【００１１】
また、$Ｘｊ＝ｇ１^{x1j}\ ｇ２^{x2j} \bmod ｐ$，$Ｙｊ＝ｇ１^{y1j}\ ｇ２^{y2j} \bmod ｐ$，$Ｚｊ＝ｇ１^{zj} \bmod ｐ$なる（Ｘ

[0011]
Moreover, let (Xj, Yj, Zj) which becomes $Xj=g1^{x1j}\ g2^{x2j} \bmod p$, $Yj=g1^{y1j}\ g2^{y2j} \bmod p$, $Zj=g1^{zj} \bmod p$
Be the decoding person's Pj public key.

ｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とする。Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z}mod ｐなる（Ｘ，Ｙ，Ｚ）を暗号化に用いる公開鍵とする。各々の復号者装置間は、安全な通信路で接続されており、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。

Let $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$mod p, and $Z=g1^{z}$ mod p be the public key which it uses for encryption (X, Y, Z).
It shall connect by the safe communication channel between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

【００１２】

Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）をCramer-Shoup 暗号方法により暗号化された平文ｍの暗号文とする。復号者装置は、協力して分散乱数生成手順を実行し、復号者Ｐｊの装置は秘密値ｒｊを得る。ここで、ｒｊは乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散した場合の、値ｗｊに対応する秘密値であり、任意のｔ＋１個の秘密値から、秘密復号手順により、ｒを回復できるような値である。また、分散乱数生成手順の性質から、各復号者装置はｒの値を知ることができず、ｒは０以上ｑ未満のランダムな整数となる。

[0012]

Let E= (u1, u2, v, e) be the cryptogram of plaintext m enciphered by the Cramer-Shoup cryptographic method.
A decoding person apparatus performs a distributed random-number generation procedure in cooperation, and the decoding person's Pj apparatus acquires the secret value rj.
Here, rj is a secret value corresponding to the value wj at the time of dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t.
It is the value which can recover r with a secret decoding procedure from the secret values of t+1 piece as desired.
Moreover, each decoding person apparatus cannot know the value of r, but r becomes the random integer of 0 or more and under q from the characteristic of a distributed random-number generation procedure.

【００１３】

[0013]

Ｅを受信した各復号者Ｐｊの装置は、ｃ＝Ｈ（ｕ１，ｕ２）およびＶｊ＝（ｕ１$^{x1j+cy1j}$ｕ２$^{x2j+cy2j}$ｖ$^{-1}$）^{rj}ｍｏｄ ｐを計算する。更に、Ｖｊをしきい値２ｔの検証可能秘密分散法により分散し、値ｗｋ（ｋ＝１，２，…，ｎ、ｋ≠ｊ）に対応する秘密値Ｖｊｋを各復号者Ｐｋの装置に安全な通信路を介して送信する。他の全ての復号者装置からＶｊｋを受信した後、復号者Ｐｋの装置はＶｋを放送型通信路を介して他の全ての復号者装置へ送信する。各復号者装置は受信した各Ｖｋが正しい値であることをＶｋｊを用いて検証する。

The apparatus of each decoding person Pj who received E are c=H (u1, u2) and Vj= (it calculates $u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1})^{rj}$mod p.).
Furthermore, it disperses Vj with a with a threshold value of 2t verifiable secret dispersion method, and transmits the secret value Vjk corresponding to a value wk (k = 1, 2..., n, k!=j) through a communication channel safe for each decoding person's Pk apparatus.
After receiving Vjk from all other decoding person apparatus, the decoding person's Pk apparatus transmits Vk to etc. of all decoding person apparatus through a broadcast type communication channel.
It verifies using Vkj that each decoding person apparatus is the value with each correct Vk which received.

【００１４】

正しいと確認されたＶｋのうち２ｔ＋１個を選択し、指数部、つまりｘ１ｋ＋ｃｙ１ｋ，ｘ２ｋ＋ｃｙ２ｋに対する秘密復元手順により復元した値Ｖが１に等しいか否かを調べる。等しくないならば他の組み合わせで同様に秘密復元手順を繰り返し、全ての２ｔ＋１個の組み合わせについていずれも復元値が１に等しくないならば、復号を拒否して停止する。

[0014]

If correct, it will choose 2t+1 piece among checked Vk(s), and it examines whether the value V decompressed by the index part, i.e., the secret decompression procedure with respect to x1k+cy1k,x2k+cy2k, is equal to 1.
These
If not equal
It repeats a secret decompression procedure similarly in other combination, and about all 2t+1 piece combination, if the decompression value is not all equal to 1, it will refuse decoding and will stop.

【００１５】

各復号者装置が上記手順に従って計算した場合、２ｔ＋１個以

[0015]

When each decoding person apparatus calculates according to the above-mentioned

上の任意の正しいＶｋから、指数部に対する秘密鍵復元手順により、Ｖ＝（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐなるＶを復元することができる。ここで、Ｖがｐを法として１と合同でないならば、Cramer-Shoup 法における本来の検証式ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$の値もｖと合同ではない。一方、Ｖが１と合同となる場合は、本来の検証式がｖと合同であるか、または、乱数ｒが０であるかのいずれかである。しかしながら、分散乱数生成手順で生成した乱数ｒが０となる確率は１／ｑであり、十分小さいので無視する事ができる。従って、Ｖが１と合同である場合には、本来の検証式はｖと合同であると見なすことができる。

procedure, from the correct Vk(s) as desired more than 2t+1 piece, the secret-key decompression procedure with respect to an index part, v= (it can decompress V used as $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p.)
Here, v should make p a method
If in cooperation with 1, also the value of original verification type $u1^{x1+cy1}u2^{x2+cy2}$ in Cramer-Shoup method
In cooperation with v.
When V becomes in cooperation with 1 on the other hand, whether an original verification type is in cooperation with v, or
Or whether a random number r is 0, it is either of this.
However, the probabilities that the random number r formed in the distributed random-number generation procedure will be set to 0 are 1/q.
Since it is small enough, it can ignore.
Therefore, when V is in cooperation with 1, it can consider in cooperation with an original verification type v.

【００１６】
ここで、不正を働く復号者が最大ｔ人いると仮定する。このｔ人は、（１）不正な暗号文Ｅに対する検証式の値Ｖが１となるようにする、または（２）正当な暗号文Ｅに対する検証式の値Ｖが１とならないようにする、の二通りの目的で上記手順から逸脱する場合があり得る。まず、（１）の目的を成功させるためには、ある２ｔ＋１個のＶｋか

[0016]
Here, it assumes that there are a maximum of t decoding persons who act irregularity.
These t persons, (1)
It makes it the value V of the verification type with respect to the irregular cryptogram E set to 1.
Or
(2)
It keeps the value V of the verification type with respect to the rightful cryptogram E from being set to 1.

ら復元されるＶの値が１となるようにしなければならない。しかしながら、不正者装置を含めた全ての復号者装置は他の復号者装置が出すＶｋの値を知る前に、自分のＶｋの値を検証可能秘密分散方法によって分散しなければならず、他の復号者装置のＶｋの値を知ってから自装置のＶｋの値を変更することはできないので、他の復号者装置のＶｋに関する予想が当たった場合のみ不正な復号者は（１）の目的を達成することができる。予想が当たる確率は１／ｑであり、十分小さいので無視することができる。次に、（２）の場合に関しては、不正な復号者装置が、どのような不正な値Ｖｋを送信したとしても、不正者は高々ｔ人であり、他の２ｔ＋１人の装置は正しい値を送信しているので、少なくとも１通りは、全て正しい値の２ｔ＋１個のＶｋから成る集合を取ることができ、そのような集合からＶ＝１が復元される。

It can deviate from the above-mentioned procedure for two kinds of these objective.
First
In order to let the objective of (1) successful, you have to make it the value of V decompressed from certain 2t+1 piece Vk set to 1.
However, all decoding person apparatus including an irregular person apparatus are before getting to know the value of Vk which another decoding person apparatus takes out, since the value of Vk of a self-apparatus cannot be altered after having to disperse the value of one's Vk with a verifiable secret dispersion method and getting to know the value of Vk of another decoding person apparatus, only when the anticipation about Vk of another decoding person apparatus comes true, an irregular decoding person can attain the objective of (1).
The probabilities that anticipation will come true are 1/q.
Since it is small enough, it can ignore.
Next, even if an irregular decoding person apparatus transmits what kind of illegitimate value Vk about the case of (2), an irregular person is at most t persons.
Other 2t+1 person apparatus have transmitted the correct value, therefore, all the at least 1 kinds can take the ensemble which constitutes of 2t+1 piece Vk of the correct value, and V= 1 is decompressed from such an ensemble.

【００１７】
情報の漏洩については、Ｖが１でない場合、どのようなｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$の値に対しても、

[0017]
About leakage of information, when V is not 1, to the value of what kind of $u1^{x1+cy1}u2^{x2+cy2}$, it is as follows.

$V=(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^r$ mod pを満たすrの値が一つ定まるので、$(u1^{x1+cy1}u2^{x2+cy2}v^{-1})$の値がrでランダム化され、このランダム化された値を示しても、rでランダム化される前の値は漏れない、つまり上記検証方法では、$u1^{x1+cy1}u2^{x2+cy2}$に関する情報は一切漏れない。

V= (one value of r which fills $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^r$ mod p becomes settled)
Therefore, the randomizing of the value of $(u1^{x1+cy1}u2^{x2+cy2}v^{-1})$ is carried out by r, even if this value by which the randomizing was carried out is shown, the value before a randomizing is carried out by r does not leak, that is, the information about $u1^{x1+cy1}u2^{x2+cy2}$ does not leak at all by the above-mentioned verification method.

【００１８】
以上より、この発明によれば、不正を働く復号者が全復号者の１／３未満ならば、秘密鍵に関する情報を一切漏らすことなく、複数復号者の協力によって本来のCramer-Shoup暗号方法の検証式と同等の検証式を計算することが可能であり、よって、適応的選択暗号文攻撃に強い、複数復号者の暗号復号装置を構成する事ができる。

[0018]
As mentioned above, without leaking the information about a secret key entirely, if the decoding person who acts irregularity according to this invention is under all decoding persons' 1/3, by cooperation of two or more decoding person, it can calculate a verification type equivalent to the verification type of an original Cramer-Shoup cryptographic method, and, therefore, can comprise two or more decoding person's code decoder strong against an adaptive choice cryptogram attack.

【００１９】
以上の手法は復号者がｎ人いる場合に、各復号者装置は、全ての復号者装置から受信したｎ個の検証用データ（Ｖ１，…，Ｖｎ）に対して、２ｔ＋１個のデータを取りだし、ある検証式を満足するか否かを検証する。満足しない場合は、この検証をｎ個に対して取り得る全ての２ｔ＋１個の組み合わせに対して行う。そのため、検証式を満足し

[0019]
When n decoding persons are in the above approach, to n data for verification (V1..., Vn) which received each decoding person apparatus from all decoding person apparatus, it takes out 2t+1 piece data, it verifies whether it satisfies a certain verification type.
When not satisfied, it performs this verification to all the 2t+1 piece combination that can be taken to n pieces.
Therefore, when not satisfying a verification type, it has the disadvantage that computational

ない場合には、復号者の数ｎに対して、計算量が指数的に増加するという欠点を持つ。

complexity increases exponentially, to several n of a decoding person.

【００２０】
この発明の別の観点によれば、複数の復号者による暗号復号方法において、多数の復号者に対しても効率的に計算が実行でき、また、１／３以上の復号者が不正を行っても回復可能であるような、適応的選択暗号文攻撃に強い暗号の暗号文検証方法およびそのプログラム記録媒体を提供する。即ちこの発明の別の観点によれば、まず、復号者の数に対する計算量を低減する手段として、零知識証明によってその結果の正当性を各復号者装置に証明させることによって不正者を特定し、正当なデータのみを用いて暗号文の検証を行う。そうすることによって、復号者の数ｎに比例した計算量で検証を行うことが可能である。しかし、この際用いる零知識証明は通信量が多いため、不正がほとんど起こらない場合には効率が悪い。各復号者装置の計算結果がＢＣＨ符号のコードワードとなるように各復号者の固有の公開値を定め、計算結果がコードワードであることを受信者装置が検証し、コードワードでない場合にのみ零知識証明を実行することによって、正しい暗

[0020]
According to another viewpoint of this invention, in the code decoding method by two or more decoding persons, it provides the cryptogram verification method and its program recording medium of a code strong against the adaptive choice cryptogram attack which can be recovered even if it can perform calculation efficiently also to many decoding people and the decoding person who is more than 1/3 performs irregularity.
That is, as means to reduce the computational complexity with respect to the number of decoding persons, by letting each decoding person apparatus prove the correctness of that result by zero knowledge proof, it specifies an irregular person and, according to another viewpoint of this invention, performs verification of a cryptogram first only using rightful data.
By doing so, it can perform verification by the computational complexity proportional to several n of a decoding person.
However, in this case, since there are many amounts of communication, the zero knowledge proof to be used is, efficiency is bad when irregularity hardly happens.
When the correct cryptogram is received by setting each decoding person's inherent open value that the calculation result of each decoding person apparatus constitutes the coding word of a BCH code, and a receiving-party apparatus verifying that a

号文を受信した場合には、通信量を抑えたまま効率的な計算を行うことが可能となる。

calculation result is the coding word, and performing zero knowledge proof only when it is not the coding word, it becomes that it is possible to perform efficient calculation, with the amount of communication restrained.

【００２１】
この方法に因れば、許容できる不正者の数は、３ｔ＋１＞ｎを満たすｔ人までであり、より許容度の高い安全なシステムが望まれる場合には不適当である。また、不正者が１／３以上１／２未満の場合に対応する手段として、不正者が特定された場合に、他の復号者装置が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるようにすることにより、課題を解決する。

[0021]
If based on this method, the number of irregular persons which can be accepted will be to t persons who fill 3t+1>n.
It is unsuitable when a safe system with a higher tolerance is desired.
Moreover, it is as means corresponding to the case where irregular persons are 1/3-1/2, another decoding person apparatus computes the distributed secret key which the irregular decoding person has in cooperation with the case where an irregular person is specified, by opening to the public, although it also becomes bored, it solves a problem by enabling it to calculate the correct result instead of the irregular decoding person.

【００２２】
具体的な手段は以下の通りである。ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊに対し、固有の公開値ｗｊを割り振る。３ｔ＜ｎを満たすしきい値ｔを定める。（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈$Ｚｑ^{5}$をしきい値ｔの秘密分散法により分散し、値ｗｊに対応する秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）を復号者Ｐｊの秘密鍵とする。

[0022]
The detailed means are as follows.
It sets n persons' decoding person to P1-Pn, and assigns the inherent open value wj to each decoding person Pj.
It defines threshold-value t which fills 3 t<n.
(x1,x2,y1,y2,z)
It disperses (element of)Zq^{5} with the secret dispersion method of threshold-value t, and let the secret value (x1 j, x2 j, y1 j, y2 j, zj) corresponding to a value wj be the decoding person's Pj secret key.

【００２３】
また、Ｘｊ＝ｇ１^{x1j} ｇ２^{x2j}mod ｐ，Ｙｊ＝ｇ１^{y1j} ｇ２^{y2j} mod ｐ，Ｚｊ＝ｇ１^{zj}mod ｐなる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とする。Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z}mod ｐなる（Ｘ，Ｙ，Ｚ）を暗号化に用いる公開鍵とする。各々の復号者装置間は、安全な通信路で接続されており、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。

[0023]
Moreover, let Xj=g1^{x1j}g2^{x2j} mod p, Yj=g1^{y1j} g2^{y2j} mod p, and Zj=g1^{zj}mod p be the decoding person's Pj public key (Xj, Yj, Zj).
Let X=g1^{x1}g2^{x2}mod p, Y=g1^{y1}g2^{y2}mod p, and Z=g1^{z} mod p be the public key which it uses for encryption (X, Y, Z).
It shall connect by the safe communication channel between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

【００２４】
Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）をCramer-Shoup 暗号方法により暗号化された平文ｍの暗号文とする。復号者装置は、協力して分散乱数生成手順を実行し、復号者Ｐｊの装置は秘密値ｒｊを得る。ここで、ｒｊは乱数ｒ∈Ｚｑをしきい値ｔの秘密分散法により分散した場合の、値ｗｊに対応する秘密値であり、任意のｔ＋１個の秘密値から、秘密復号手順により、ｒを回復できるような値である。また、分散乱数生成手順の性質から、各復号者はｒの値を知ることができず、ｒは０以上ｑ未満のランダムな整数となる。

[0024]
Let E= (u1, u2, v, e) be the cryptogram of plaintext m enciphered by the Cramer-Shoup cryptographic method.
A decoding person apparatus performs a distributed random-number generation procedure in cooperation, and the decoding person's Pj apparatus acquires the secret value rj.
Here, rj is a secret value corresponding to the value wj at the time of dispersing random-number r(element of)Zq with the secret dispersion method of threshold-value t.
It is the value which can recover r with a secret decoding procedure from the secret values of t+1 piece as desired.
Moreover, each decoding person cannot know the value of r, but r becomes the random integer of 0 or more and under q from the characteristic

of a distributed random-number generation procedure.

【００２５】
次に、全復号者装置は協力して分散乗算手段を実行し、各復号者Ｐｊの装置は秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′を得る。ここで、秘密値ｘ１ｊ′は、乱数ｒと秘密鍵ｘ１の積をしきい値ｔの秘密分散法により分散して得られる値であり、任意のｔ＋１人の復号者が持つｘ１ｊ′から、ｒ・ｘ１（mod ｑ）を復号することが可能である。秘密値ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′についても同様に、それぞれ任意のｔ＋１個の値から、ｒ・ｘ２（mod ｑ），ｒ・ｙ１（mod ｑ），ｒ・ｙ２（mod ｑ）を復元することができる。

[0025]
Next, all decoding person apparatus cooperate and perform distributed multiplication means, each decoding person's Pj apparatus obtains secret value x1j',x2j',y1j',y2j'.
Here, secret value x1j' is a value obtained by dispersing the product of a random number r and a secret key x1 with the secret dispersion method of threshold-value t.
It can decode x1j' to r-x1 (mod q) which t+1 person's decoding persons as desired have.
It can decompress r-x2 (mod q), r-y1 (mod q), and r-y2 (mod q) from the values of t+1 piece respectively as desired similarly about secret value x2j', y1j', and y2j'.

【００２６】
Ｅを受信した各復号者Ｐｊ装置は、ｃ＝Ｈ（ｕ１，ｕ２）およびＶｊ＝ｕ１$^{x1j'+cy1j'}$ｕ２$^{x2j'+cy2j'}$ｖ$^{-rj}$mod ｐを計算し、放送型通信路を通じて他の全ての復号者装置へＶｊを送信する。次に、各復号者装置は、（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する。（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードでなく、正しくないことが判明し

[0026]
Each decoding person Pj apparatus which received E, it calculates c=H(u1,u2) and Vj=u1$^{x1j'+cy1j'}$u2$^{x2j'+cy2j'}$v^{-rj} mod p, it transmits Vj to all other decoding person apparatus through a broadcast type communication channel.
Next, each decoding person apparatus checks that the index part of (V1..., Vn) is the coding word of a BCH code.
The index part of (V1..., Vn) is not the coding word of a BCH code, when it becomes clear that it is not correct, it is each decoding person's Pj apparatus, it proves to another decoding

た場合、各復号者Ｐｊの装置は、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod ｐの計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者に証明する。

person by zero knowledge proof, without leaking the information concerning [that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj}$ mod p, and] x1j',x2j',y1j',y2j',rj.

【００２７】

証明に失敗した復号者Ｐｊは不正者であると見なされ、その不正者である逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを他の復号者装置が秘密値回復手順を用いて回復し、正しいＶｊの値を公開する。公開された正しいＶｊの値を含めて、正しい（Ｖ１，…，Ｖｎ）を得る。（Ｖ１，…，Ｖｎ）の指数部が正しいこと、コードワードであることを確認した後、指数部に対する秘密復元手順により、値Ｖを復元する。各復号者装置はＶが１に等しいか否かを調べ、等しくないならば復号を拒否して停止する。

[0027]

It considers that the decoding person Pj who failed in proof is an irregular person, another decoding person apparatus recovers secret value x1j',x2j',y1j',y2j',rj of the deviation person who is the irregular person using a secret value recovery procedure, and it exhibits the correct value of Vj.

It includes the exhibited correct value of Vj, it obtains correct (V1..., Vn).

After the index part of (V1..., Vn) checks the correct thing and that it is the coding word, it decompresses a value V with the secret decompression procedure with respect to an index part.

Each decoding person apparatus

It examines whether V is equal to 1, if not equal, it will refuse decoding and will stop.

【００２８】

等しいならば、各復号者Ｐｊの装置は$Dj=u1^{zj} \bmod p$を計算し、放送型通信路により他の全ての復号者装置へ送信する。Ｄｊを受信した各復号者装置は（Ｄ１，…，Ｄｎ）に対して、（Ｖ１，…，Ｖｎ）に対して行

[0028]

If these etc. come to be by carrying out, each decoding person's Pj apparatus

It calculates $Dj=u1^{zj} \bmod p$, it transmits to all other decoding person apparatus according to a broadcast type communication channel.

When verification of the coding word similar to having carried out to (V1..., Vn) is performed to

ったのと同様のコードワードの検証を行い、不正を検出した場合には同様に零知識証明を行って不正者を特定し、正しいＤｊの値を秘密値回復手順を用いて回復する。

【００２９】
各復号者装置は、正しい（Ｄ１，…，Ｄｎ）から、指数部に対する秘密復元手順によってＤ＝ｕ１^{z} mod ｐを復元し、ｍ＝ｅ／Ｄmod ｐを計算してメッセージｍを復号する。各復号者装置が上記手順に従って計算した場合、２ｔ＋１個以上の任意の正しいＶｋから、指数部に対する秘密鍵復元手順により、Ｖ＝（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐなるＶを復元することができる。ここで、Ｖがｐを法として１と合同でないならば、Cramer-Shoup 法における本来の検証式ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$の値もｖと合同ではない。一方、Ｖが１と合同となる場合は、本来の検証式がｖと合同であるか、または、乱数ｒが０であるかのいずれかである。しかしながら、分散乱数生成手順で生成した乱数ｒが０となる確率は１／ｑであり、十分小さいので無視する事ができる。従って、Ｖが１と合同である場合には、本来の検証式はｖと合同であると見なすことができる。

(D1..., Dn) and irregularity is detected, each decoding person apparatus which received Dj performs zero knowledge proof similarly, specifies an irregular person, and recovers the correct value of Dj using a secret value recovery procedure.

[0029]
From it being correct (D1..., Dn), with the secret decompression procedure with respect to an index part, each decoding person apparatus decompresses $D=u1^{z}$ mod p, calculates m=e/Dmod p, and decodes Message m.
When each decoding person apparatus calculates according to the above-mentioned procedure, from the correct Vk(s) as desired more than 2t+1 piece, the secret-key decompression procedure with respect to an index part, it can decompress V used as $V=(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p.
Here, if V makes p a method.
And is not in cooperation with 1, also the value of original verification type $u1^{x1+cy1}u2^{x2+cy2}$ in Cramer-Shoup method
In cooperation with v.
On the other hand, when V becomes in cooperation with 1, whether in cooperation with an original verification type v, or
Whether a random number r is 0.
It is either of this.
However, the probabilities that the random number r formed in the distributed random-number generation procedure will be set to 0 are 1/q.
Since it is small enough, it can ignore.
Therefore, when V is in cooperation with 1, it

can consider in cooperation with an original verification type v.

【００３０】
ここで、不正を働く復号者が最大ｔ人いると仮定する。このｔ人は、（１）不正な暗号文Ｅに対する検証式の値Ｖが１となるようにする、または（２）正当な暗号文Ｅに対する検証式の値Ｖが１とならないようにする、の二通りの目的で上記手順から逸脱する場合があり得る。しかしながら、全ての復号者装置の出力はＢＣＨ符号のコードワード検査によって検証されるため、不正な値が存在する場合は、不正な値が全体の１／３未満ならば、その存在を検知することができる。そのような場合には、各々の復号者は零知識証明により出力値の正しさを証明するので、不正な値を出力した不正者は証明に失敗し、排除される。

[0030]
Here, it assumes that there are a maximum of t decoding persons who act irregularity.
These t persons, (1)
It makes it the value V of the verification type with respect to the irregular cryptogram E set to 1.
Or
(2)
It keeps the value V of the verification type with respect to the rightful cryptogram E from being set to 1.
It can deviate from the above-mentioned procedure for two kinds of these objective.
However, the output of all decoding person apparatus can detect the presence, if an illegitimate value is under whole 1/3 when an illegitimate value exists since it is verified by the coding word inspection of a BCH code.
In such a case, each decoding person proves the rightness of an output value by zero knowledge proof, therefore, the irregular person who outputted the illegitimate value fails in proof, it is eliminated.

【００３１】
情報の漏洩については、Ｖが１でない場合、どのようなｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$の値に対しても、Ｖ＝（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod ｐを満たすｒの値が一つ定まるので、上記検証方法では、ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$に関する情

[0031]
About leakage of information
When V is not 1, to the value of what kind of $u1^{x1+cy1}u2^{x2+cy2}$, it is as follows.
V= (one value of r which satisfies $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p becomes settled)
Therefore, by the above-mentioned verification method, the information about $u1^{x1+cy1}u2^{x2+cy2}$

報は一切漏れない。以上より、この発明によれば、不正を働く復号者が全復号者の１／３未満ならば、秘密鍵に関する情報を一切漏らすことなく、複数復号者の協力によって本来のCramer-Shoup 暗号方法の検証式と同等の検証式を計算することが可能であり、よって、適応的選択暗号文攻撃に強い、複数復号者の暗号復号方法を構成する事ができる。

does not leak at all.
As mentioned above, without leaking the information about a secret key entirely, if the decoding person who acts irregularity according to this invention is under all decoding persons' 1/3, by cooperation of two or more decoding person, it can calculate a verification type equivalent to the verification type of an original Cramer-Shoup cryptographic method, and, therefore, can comprise two or more decoding person's code decoding method strong against an adaptive choice cryptogram attack.

【００３２】
一方、上記手段において、ＢＣＨ符号のコードワード検査を行わず、常に零知識証明を実行して不正者を特定し、他の復号者が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるので、１／２未満の不正者に対応することができる（零知識証明が正しいことは多数決で決定するため、少なくとも１／２の復号者は正しくなければならない）。

[0032]
On the other hand, for the above-mentioned means, it does not conduct the coding word inspection of a BCH code, it always performs zero knowledge proof and specifies an irregular person, it computes the distributed secret key which another decoding person cooperates and the irregular decoding person has, it opens to the public, although it also becomes bored, instead of the irregular decoding person, the correct result is calculable, therefore, it can respond to the irregular person of under 1/2 (in order to decide by majority that zero knowledge proof is correct, the decoding person of 1/2 at least must be correct).

【００３３】

[0033]

【発明の実施の形態】
実施例１
以下に、この発明の第一の実施例である暗号文検証方法につい

[EMBODIMENT OF THE INVENTION]
Example 1
Below, it demonstrates the cryptogram verification method which is the first Example of

て説明する。図１に示すように暗号文作成者装置１１で作成された暗号文は復号者装置１２で復号される。復号者装置１２で、正しい暗号文でないと、勝手に復号拒否することを避けるため、検証者装置１３で、復号拒否が妥当なものであるか否かを検証する。

this invention.
The cryptogram made with the cryptogram maker apparatus 11 as shown in FIG. 1 is decoded with the decoding person apparatus 12.
If it is not the correct cryptogram with the decoding person apparatus 12, in order to avoid carrying out decoding refusal voluntarily, it verifies whether decoding refusal is appropriate with the verification person apparatus 13.

【００３４】
いま大きな素数ｐ，ｑがあり、ｑはｐ－１を割り切るものとする。Ｇｑの元ｇ１，ｇ２をランダムに選択する。Ｘ＝ｇ１^{x1}ｇ２^{x2}mod ｐ，Ｙ＝ｇ１^{y1}ｇ２^{y2}mod ｐ，Ｚ＝ｇ１^{z}mod ｐを暗号化手順に用いる公開鍵とする。ここで、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）∈Ｚｑ^{5}とする。公開鍵は公開パラメータめとしてｐ，ｑ，ｇ１，ｇ２と共に公開されているものとする。また秘密鍵は復号者装置のメモリ上に格納されているものとする。

[0034]
There are big prime numbers p and q now.
Q shall give a clear-cut solution to p-1.
It chooses the origin g1 and g2 of Gq at random.
Let $X=g1^{x1}g2^{x2}$mod p, $Y=g1^{y1}g2^{y2}$mod p, and $Z=g1^{z}$ mod p be the public key which it uses for an encryption procedure.
Here, it considers it as (x1,x2,y1,y2,z)(element of)Zq^{5}.
Public key shall be exhibited with p, q, g1, and g2 as an open parameter.
Moreover, the secret key shall be stored on the memory of a decoding person apparatus.

【００３５】
Ｘ，Ｙ，Ｚを公開鍵としたCramer-Shoup 暗号方法により暗号化された平文ｍの暗号文Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を図２に示すように受信した後（Ｓ１）、復号者装置は、乱数ｒを生成し（Ｓ２）、ｃ＝Ｈ（ｕ１，ｕ２）およびＶ＝（ｕ１$^{x1+cy1}$ｕ２

[0035]
After, receiving cryptogram E= (u1, u2, v, e) of plaintext m enciphered by the Cramer-Shoup cryptographic method which used X, and Y and Z as public key as shown in FIG. 2, (S1) and a decoding person apparatus form a random number r, and they are (S2), c=H (u1, u2), and V= ((S3) which calculates $u1^{x1+cy1}u2^{x2+cy2}v^{-1})^{r}$ mod p.).

$^{x2+cy2}$ v $^{-1}$) ^{r} mod pを計算する（Ｓ３）。Ｖが１ならば、この暗号文を合格とし（Ｓ４）、復号計算を行う（Ｓ５）。

If V becomes one, it will consider this cryptogram as a pass and will perform (S4) and decoding calculation (S5).

【００３６】

Ｖが１でないならば不合格とする。第三者へ不合格であることを証明するため、ビットコミットメント関数ＢＣ（）を用いて、ＢＣ（ｒ）を公開する。このビットコミット関数には、たとえば、Ｐｅｄｅｒｓｅｎによるものがある。即ち、乱数ｓを生成し、ＢＣ（ｒ，ｓ）：＝$g^r h^s$ mod pと計算する。ここでｇ，ｈはｇを底とするｈの離散対数が未知であるようなＧｑの元である。

[0036]

If V is not 1, it will consider it as a rejection.
In order to prove that it is a rejection to a third person, it uses bit commitment function BC(), it exhibits BC (r).
There are some which are depended on Pedersen in this bit commitment function, for example.
That is, it forms a random number s, it calculates with $BC(r, s):=g^r h^s \bmod p$.
G and h are here under Gq whose discrete logarithm of h which uses g as a bottom is unknown.

【００３７】

その後、ＢＣ（ｒ，ｓ）を構成するｒと、公開鍵Ｘ，Ｙを構成するｘ１，ｘ２，ｙ１，ｙ２を用いて（ｕ１$^{x1+cy1}$ｕ２$^{x2+cy2}$ｖ$^{-1}$）^{r} mod pなる計算を行った結果がＶであることを、ｒ，ｘ１，ｘ２，ｙ１，ｙ２に関する秘密を漏らさずに、零知識証明で第三者へ証明する（Ｓ６）。この零知識証明は、以下の手順で行う。

[0037]

After that, r which comprises BC(r,s), it comprises public-key X,Y.
Use x1,x2,y1,y2.
The result of having performed calculation used as $(u1^{x1+cy1}u2^{x2+cy2}v^{-1})^r \bmod p$ is V, it proves to a third person by zero knowledge proof, without leaking the secret about r,x1,x2,y1,y2 (S6).
The following procedures perform this zero knowledge proof.

【００３８】

以下では、ｇ，ｈを、ｇを底とするｈの離散対数が未知であるようなＧｑの元とする。復号者

[0038]

Below, it carries out g and h the origin of Gq whose discrete logarithm of h which uses g as a bottom is unknown.

装置は、乱数ａ，ａ１，ａ２，ｂ１，ｂ２をＺｑより選択し、
$R = g^{r} h^{a} \bmod p$
$RX1 = R^{x1} h^{a1} \bmod p$
$RX2 = R^{x2} h^{a2} \bmod p$

$RY1 = R^{y1} h^{b1} \bmod p$
$RY2 = R^{y2} h^{b2} \bmod p$
なるＲ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を検証者装置へ送付する。

A decoding person apparatus chooses random numbers a, a1, a2, b1, and b2 from Zq, $r=g^{r}h^{a} \bmod p$
$RX1=R^{x1}h^{a1} \bmod p$
$RX2=R^{x2}h^{a2} \bmod p$

$RY1=R^{y1}h^{b1} \bmod p$
$RY2=R^{y2}h^{b2} \bmod p$
It sends R,RX1,RX2,RY1,RY2 used as this to a verification person apparatus.

【００３９】
さらに、復号者装置は乱数ｗ０をＺｑよりランダムに選択し、
$K = g$, $L = g^{w0} \bmod p$
を検証者装置へ送付する。検証者装置は、ｅ０およびｅ１をＺｑよりランダムに選択して
$B = K^{e0} L^{e1} \bmod p$

を計算してＢを復号者装置へ送付する。

[0039]
Furthermore, a decoding person apparatus chooses a random number w0 from Zq at random, $k=g$, $L=g^{w0} \bmod p$
It sends these to a verification person apparatus.
A verification person apparatus chooses e0 and e1 from Zq at random.
$B=K^{e0}L^{e1} \bmod p$

It calculates these and sends B to a decoding person apparatus.

【００４０】
復号者装置は乱数ｗ１～ｗ１８をＺｑよりランダムに選択し、
$T_1 = g_1^{w1} g_2^{w2} \bmod p$
$T_2 = g_1^{w3} g_2^{w4} \bmod p$
$T_3 = g^{w5} g^{w6} \bmod p$

$T_4 = R^{w1} h^{w7} \bmod p$
$T_5 = R^{w2} h^{w8} \bmod p$
$T_6 = R^{w3} h^{w9} \bmod p$
$T_7 = R^{w4} h^{w10} \bmod p$

[0040]
A decoding person apparatus chooses random-number w1-w18 from Zq at random, $t_1 = g_1^{w1} g_2^{w2} \bmod p$
$T_2=g_1^{w3}g_2^{w4} \bmod p$
$T_3=g^{w5}g^{w6} \bmod p$

$T_4=R^{w1}h^{w7} \bmod p$
$T_5=R^{w2}h^{w8} \bmod p$
$T_6=R^{w3}h^{w9} \bmod p$
$T_7=R^{w4}h^{w10} \bmod p$

$T_8 = g^{w11}\ h^{w12} \bmod p$
$T_9 = g^{w13}\ h^{w14} \bmod p$
$T_{10} = g^{w15}\ h^{w16} \bmod p$
$T_{11} = g^{w17}\ h^{w18} \bmod p$

$T_{12} = u1^{w11+cw15} u2^{w13+cw17} v^{-w5} \bmod p$
を計算して、検証者装置へ送付する。

$T_8 = g^{w11} h^{w12} \bmod p$
$T_9 = g^{w13} h^{w14} \bmod p$
$T_{10} = g^{w15} h^{w16} \bmod p$
$T_{11} = g^{w17} h^{w18} \bmod p$

$T_{12} = u1^{w11+cw15} u2^{w13+cw17} v^{-w5} \bmod p$
It calculates these and sends to a verification person apparatus.

【００４１】
検証者装置は、ｅ０，ｅ１を復号者装置へ送付する。
復号者装置は、$B = K^{e0} L^{e1} \bmod p$
が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、復号者装置は
$z1 = w1 + e0 \cdot x1 \bmod q$

$z2 = w2 + e0 \cdot x2 \bmod q$
$z3 = w3 + e0 \cdot y1 \bmod q$
$z4 = w4 + e0 \cdot y2 \bmod q$
$z5 = w5 + e0 \cdot r \bmod q$

$z6 = w6 + e0 \cdot a \bmod q$
$z7 = w7 + e0 \cdot a1 \bmod q$

[0041]
A verification person apparatus sends e0 and e1 to a decoding person apparatus.
A decoding person apparatus is $B = K^{e0} L^{e1} \bmod p$.
It checks that these are formed, it stops proof, when not formed.
When this is formed, it is a decoding person apparatus.
Z1=w1+e0 and x1 modq

Z2=w2+e0 and x2 modq
Z3=w3+e0 and y1 modq
Z4=w4+e0 and y2 modq
Z5=w5+e0andr modq

Z6=w6+e0anda modq
Z7=w7+e0 and a1 modq
Z8=w8+e0 and a2 modq
Z9=w9+e0 and b1 modq

z 8＝w 8＋e 0・a 2 mod q
z 9＝w 9＋e 0・b 1 mod q

z 10＝w 10＋e 0・b 2 mod q
z 11＝w 11＋e 0・r・x 1 mod q
z 12＝w 12＋e 0（a・x 1＋a 1） mod q
z 13＝w 13＋e 0・r・x 2 mod q

z 14＝w 14＋e 0（a・x 2＋a 2） mod q
z 15＝w 15＋e 0・r・y 1 mod q
z 16＝w 16＋e 0（a・y 1＋b 1） mod q
z 17＝w 17＋e 0・r・y 2 mod q

z 18＝w 18＋e 0（a・y 2＋b 2） mod q
を計算してｚ１～ｚ１８およびｗ０を検証者装置へ送付する。

Z10=w10+e0 and b2 modq
Z11=w11+e0 and r-x1 modq
Z12=w12+e0 (a-x1+a1) modq
Z13=w13+e0 and r-x2 modq

Z14=w14+e0 (a-x2+a2) modq
Z15=w15+e0 and r-y1 modq
Z16=w16+e0 (a-y1+b1) modq
Z17=w17+e0 and r-y2 modq

Z18=w18+e0 (a-y2+b2) modq
It calculates these and sends z1-z18 and w0 to a verification person apparatus.

【００４２】
検証者装置は、
$L = g^{w0} \bmod p$
$g_1^{z1} g_2^{z2} = T_1 X^{e0} \bmod p$
$g_1^{z3} g_2^{z4} = T_2 Y^{e0} \bmod p$

$g^{z5} h^{z6} = T_3 R^{e0} \bmod p$
$R^{z1} h^{z7} = T_4 (RX1)^{e0} \bmod p$

[0042]
Verification person apparatus, $I=g^{w0}$ modp
$G_1^{z1} g_2^{z2} = T_1 X^{e0} \bmod p$
$G_1^{z3} g_2^{z4} = T_2 Y^{e0} \bmod p$

$G^{z5} h^{z6} = T_3 R^{e0}$ modp
$R^{z1} h^{z7} = T_4 (RX1)^{e0} \bmod p$

p
$R^{z2}h^{z8}=T_5\ (RX2)^{e0}\mathrm{mod}$ p
$R^{z3}h^{z9}=T_6\ (RY1)^{e0}\mathrm{mod}$ p

$R^{z2}h^{z8}=T_5$ （ＲＸ２）^{e0}mod p
$R^{z3}h^{z9}=T_6$ （ＲＹ１）^{e0}mod p

$R^{z4}h^{z10}=T_7\ (RY2)^{e0}\mathrm{mod}$ p
$G^{z11}h^{z12}=T_8\ (RX1)^{e0}\mathrm{mod}$ p
$G^{z13}h^{z14}=T_9\ (RX2)^{e0}\mathrm{mod}$ p
$G^{z15}h^{z16}=T_{10}(RY1)^{e0}\mathrm{mod}$ p

$R^{z4}h^{z10}=T_7$ （ＲＹ２）^{e0}mod p
$g^{z11}h^{z12}=T_8$ （ＲＸ１）^{e0}mod p
$g^{z13}h^{z14}=T_9$ （ＲＸ２）^{e0}mod p
$g^{z15}h^{z16}=T_{10}$ （ＲＹ１）^{e0}mod p

$G^{z17}h^{z18}=T_{11}(RY2)^{e0}\mathrm{mod}$ p
$U1^{z11+cz15}u2^{z13+cz17}v^{-z5}=T_{12}V^{e0}\mathrm{mod}$ p
It verifies that these are formed.

$g^{z17}h^{z18}=T_{11}$ （ＲＹ２）^{e0}mod p
$u1^{z11+cz15}u2^{z13+cz17}v^{-z5}=T_{12}V^{e0}$mod p
が成り立つことを検証する。

【００４３】
上の証明の原理は、Schnorr 署名と同様であり、復号者装置がＶ，Ｘ，Ｙ，Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を正しく作成した場合にのみ検証式が成り立つので、一つでも成り立たない場合は検証を失敗とする。

[0043]
The principle of the upper proof is Schnorr. It is the same as that of a signature.
Since a verification type is formed only when a decoding person apparatus makes correctly V, X, and Y, R, RX1, RX2, RY1 and RY2, when at least one is not formed, it considers verification as failure.

【実施例２】
以下に、この発明の第二の実施例について説明する。図３に示すように暗号作成者装置１１と復号者Ｐ１～Ｐｎの各装置12_1～12_nとは放送型通信路１

[EXAMPLE 2]
Below, it demonstrates the 2nd Example of this invention.
As shown in FIG. 3, the code maker apparatus 11, and each apparatus 12_1-12_n of decoding person P1-Pn are connected to the broadcast

４に接続され、また復号者装置１２$_1$～１２$_n$は相互に安全な通信路１５で接続されている。

type communication channel 14, moreover, decoding person apparatus 12_1 -12_n is connected by the mutually safe communication channel 15.

【００４４】

いま大きな素数ｐ，ｑがあり、ｑはｐ－１を割り切るものとする。Ｇｑの元ｇ１，ｇ２をランダムに選択する。まず、ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊ（ｊ＝１，２，…，ｎ）に対し、固有の公開値ｗｊを割り振る。３ｔ＜ｎを満たすしきい値ｔを定める。全復号者装置は、しきい値ｔの分散乱数生成手順を３回実行し、復号者Ｐｊの装置は秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）を得、これを復号者Ｐｊの秘密鍵とする。また、$Xj=g1^{x1j}g2^{x2j} \bmod p$，$Yj=g1^{y1j}g2^{y2j} \bmod p$，$Zj=g1^{zj} \bmod p$なる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とする。さらに、$X=g1^{x1}g2^{x2} \bmod p$，$Y=g1^{y1}g2^{y2} \bmod p$，$Z=g1^{z} \bmod p$を暗号化手順に用いる公開鍵とする。ここで、（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）$\in Zq^5$は任意のｔ＋１組の秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）から、秘密復元手順により復元される乱数である。このような乱数を生成する分散乱数生成手順には、例えば、

[0044]

There are big prime numbers p and q now.

Q shall give a clear-cut solution to p-1.

It chooses the origin g1 and g2 of Gq at random.

First, it sets n persons' decoding person to P1-Pn, to each decoding person Pj (j = 1, 2..., n) It assigns the inherent open value wj.

It defines threshold-value t which fills 3 t<n.

All decoding person apparatus perform the distributed random-number generation procedure of threshold-value t 3 times, the decoding person's Pj apparatus acquires a secret value (x1 j, x2 j, y1 j, y2 j, zj), let this be the decoding person's Pj secret key.

Moreover, let $Xj=g1^{x1j}g2^{x2j} \bmod p$, $Yj=g1^{y1j}g2^{y2j} \bmod p$, and $Zj=g1^{zj} \bmod p$ be the decoding person's Pj public key (Xj, Yj, Zj).

Furthermore, let $X=g1^{x1}g2^{x2} \bmod p$, $Y=g1^{y1}g2^{y2} \bmod p$, and $Z=g1^{z} \bmod p$ be the public key which it uses for an encryption procedure.

Here, (x1,x2,y1,y2,z)(element of)Zq^5 is a random number decompressed by a secret decompression procedure from t+1 set of secret values (x1 j, x2 j, y1 j, y2 j, zj) as desired.

There is the method of depending on Pedersen in the number generation procedure of part scattering which forms such a random number, for example.

Below, the distributed random-number

Ｐｅｄｅｒｓｅｎによる方法がある。以下に、その分散乱数生成手順を示す。

generation procedure is shown.

【００４５】

各々の復号者装置間には、図３に示したように安全な通信路１５があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路１４を利用できるものとする。

Ｓ－１）Ｐｊの装置はＺｑ上の二つの多項式ｆ（Ｘ）＝a_{0j}＋a_{1j}Ｘ＋…＋$a_{tj}X^t$およびg_j（Ｘ）＝b_{0j}＋b_{1j}Ｘ＋…＋$b_{tj}X^t$をランダムに選択し、各Ｐｋの装置（ｋ＝１，２，…，ｎ、ｋ＝ｊを除く）へｆｊ（ｗｋ）およびｇｊ（ｗｋ）を安全な通信路を通じて送信する。

[0045]

As shown in FIG. 3, the safe communication channel 15 shall be between each decoding person apparatus, and each decoding person apparatus shall utilize the broadcast type communication channel 14 it is guaranteed to be to receive the content with all the members' same other decoding person apparatus.

S-1)

The apparatus of Pj chooses two polynomial $f(X)=a_{0j}+a_{1j}X+...+a_{tj}X^t$ and, and $g_j(X)=b_{0j}+b_{1j}X+...+b_{tj}X^t$ on Zq at random, it transmits fj (wk) and gj (wk) to each apparatus (k = except for 1, 2..., n, and k=j) of Pk through a safe communication channel.

【００４６】

Ｓ－２）Ｐｊの装置はｉ＝１，…，ｔに対して$C_{ij}=g1^{aij}\ g2^{bij} \bmod p$を計算し、放送型通信路を通じて他の全ての復号者装置へ送信する。

Ｓ－３）他の全ての復号者装置からC_{ij}を受信したＰｋの装置は$wki=wk^i \bmod q$として$g1^{fj(wk)}\ g2^{gj(wk)}=C_{0j}^{wk0}\cdot C_{1j}^{wk1}\cdots C_{tj}^{wkt} \bmod p$が成り立つことを検証する。

[0046]

S-2)

The apparatus of Pj should receive i= 1..., t.

It calculates $C_{ij}=g1^{aij}\ g2^{bij} \bmod p$, it transmits to all other decoding person apparatus through a broadcast type communication channel.

S-3) The apparatus of Pk which received C_{ij} from all other decoding person apparatus verifies that $g1^{fj(wk)}g2^{gj(wk)}=C_{0j}^{wk0}*C_{1j}^{wk1}\ ...C_{tj}^{wkt} \bmod p$ is formed as $wki=wk^i \bmod q$.

【００４７】

[0047]

Ｓ－４）Ｐｋの装置はｘ１ｋ＝ｆ１（ｗｋ）＋ｆ２（ｗｋ）＋…＋ｆｎ（ｗｋ）mod ｑ、ｘ２ｋ＝ｇ１（ｗｋ）＋ｇ２（ｗｋ）＋…＋ｇｎ（ｗｋ）mod ｑとして分散乱数値ｘ１ｋ，ｘ２ｋを得る。

S-4) The apparatus of Pk obtains distributed random-number value x1k,x2k as x1k=f1(wk)+f2(wk)+...+fn(wk)mod q,x2k=g1(wk)+g2(wk)+...+gn(wk)mod q.

Ｓ－５）Ｘ＝Ｃ$_{00}$・Ｃ$_{01}$…Ｃ$_{0n}$ mod ｐとする。同様に公開鍵Ｙ，Ｚおよび各復号者の対応する秘密鍵ｙ１ｊ，ｙ２ｊ，ｚｊも同様に作成する。

S-5) It considers it as $X=C_{00}*C_{01}...C_{0n}$ modp. It also makes similarly secret-key y1j, y2j, and zj to which public key Y and Z and each decoding person correspond similarly.

【００４８】

全復号者装置は、分散乱数生成手順によって、分散された乱数ｒ∈Ｚｑを生成し、各復号者Ｐｊの装置は秘密値ｒｊを保持する（図５，Ｓ１）。Ｘ，Ｙ，Ｚを公開鍵としたCramer-Shoup暗号方法により暗号化された平文ｍの暗号文Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を受信した後（Ｓ２）、各復号者Ｐｊの装置は、ｃ＝Ｈ（ｕ１，ｕ２）およびＶｊ＝（ｕ１$^{x1j+cy1j}$ｕ２$^{x2j+cy2j}$ｖ$^{-1}$）^{rj}mod ｐを計算する（Ｓ３）。

[0048]

All decoding person apparatus form dispersed random-number r(element of)Zq with a distributed random-number generation procedure, and each decoding person's Pj apparatus maintains the secret value rj (FIG. 5, S1).

After receiving cryptogram E=(u1,u2,v,e) of plaintext m enciphered by the Cramer-Shoup cryptographic method which used X,Y,Z as public key, the apparatus of (S2) and each decoding person Pj are c=H (u1, u2) and Vj= ((S3) which calculates $u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1})^{rj}$mod p.).

【００４９】

続いてＰｊの装置はＶｊをしきい値２ｔの検証可能秘密分散法により分散し、値ｗｋに対応する秘密値Ｖｊｋを各復号者Ｐｋの装置に安全な通信路を介して送信する（Ｓ４）。ここで用いる検証可能秘密分散法には、Ｐｅ

[0049]

Then, the apparatus of Pj disperses Vj with a with a threshold value of 2t verifiable secret dispersion method, and it transmits the secret value Vjk corresponding to a value wk through a communication channel safe for each decoding person's Pk apparatus (S4).

It can use the method of Pedersen for the

ｄｅｒｓｅｎの方法を用いることができる。以下はその手順である。

Ｐ－１）大きな素数Ｐ，Ｑがあり、ＱはＰ－１を割り切り、またＱ＞ｐとする、ｇおよびｈは、$\log_g h$の値が未知であるようなG_Qの元とする。

verifiable secret dispersion method which it uses here.

The following is the procedure.

P-1) There are big prime numbers P and Q. G and h which Q gives a clear-cut solution to P-1, and it makes into Q>p are the origin of G_Q whose value of $\log_g h$ is unknown.

【００５０】

Ｐ－２）Ｐｊの装置はZ_Q上の二つの多項式$f_j(X)=V_j+a_{1j}X+\cdots+a_{tj}X^t$および$g_j(X)=b_{0j}+b_{1j}X+\cdots+b_{tj}X^t$（ただし$a_{0j}=Vj$とする）をＶｊの部分を除いてランダムに選択し、各Ｐｋの装置へｆｊ（ｗｋ）およびｇｊ（ｗｋ）、つまりＶｊｋを安全な通信路を通じて送信する。

Ｐ－３）Ｐｊの装置はｉ＝１，…，ｔに対して$C_{ij}=g^{aij}h^{bij} \bmod p$を計算し、放送型通信路を通じて他の全ての復号者装置へ送信する。

[0050]

P-2)

The apparatus of Pj

Two polynomial $f_j(X)=V_j+a_{1j}X+...+a_{tj}X^t$ and, $g_j(X)=b_{0j}+b_{1j}X+...+b_{tj}X^t$ on Z_Q

(However, it is referred to as $a_{0j}=Vj$)

Except for the part of V_j, it chooses this at random, it transmits fj (wk) and gj (wk), i.e., Vjk, to each apparatus of Pk through a safe communication channel.

P-3)

The apparatus of Pj should receive i= 1..., t.

It calculates $C_{ij}=g^{aij}h^{bij} \bmod p$, it transmits to all other decoding person apparatus through a broadcast type communication channel.

【００５１】

Ｐ－４）C_{ij}を受信したＰｋの装置はｗｋｉ＝ｗｋ^i mod ｑとして$g^{fj(wk)}h^{gj(wk)}=C_{0j}^{wk0}\cdot C_{1j}^{wk1}\cdots C_{tj}^{wkt} \bmod p$が成り立つことを検証する、つまりＶｊｋを検証する（Ｓ５）。

Ｐ－５）成り立たない場合、Ｐｋの装置は「不合格」を放送型通信路を通じて他の全ての復号

[0051]

The apparatus of Pk which received P-4 C_{ij} verifies that $g^{fj(wk)}h^{gj(wk)}=C_{0j}^{wk0}*C_{1j}^{wk1}...C_{tj}^{wkt} \bmod p$ is formed as wki=wk^i mod q, that is, verifies Vjk (S5).

P-5)

When not formed, the apparatus of Pk transmits a "rejection" to all other decoding person apparatus through a broadcast type communication channel.

者装置へ送信する。

【００５２】
Ｐ－６）「不合格」通知がｔ＋１個以上である場合、Ｐｊは不正者と見なされて排除され（Ｓ６）、他の全復号者装置はＰｊの装置が以前に送信した全ての情報を廃棄する。Ｐ－４，５，６のステップは分散秘密値Ｖｊｋの検証と、不正者の排除を行う手順であり、全ての復号者装置がデータを送信し終わった後、まとめて不合格リストを公表することで行ってもよい。

[0052]
P-6)
When the notification of a "rejection" is t+1 or more pieces, it is regarded as an irregular person, and is eliminated and Pj is (S6), other all decoding person apparatus
The apparatus of Pj aborts all the information transmitted before.
The step of P-s 4, 5, and 6 is the procedure of performing verification of the distributed secret value Vjk, and an irregular person's rejection.
After all decoding person apparatus finish transmitting data, it is sufficient to carry out by releasing a rejection list collectively.

【００５３】
全復号者装置が上記手順によってＶｊを分散した後、各復号者Ｐｊの装置は、Ｖｊおよびb_{0j}を放送型通信路を通じて他の全ての復号者装置へ送信する（Ｓ７）。これを受信した各復号者Ｐｊの装置は、$C_{0j}=g1^{Vj}h^{b0j} \bmod p$が成り立つことを確認してＶｊを検証する（Ｓ８）。成り立たない場合は、前記同様、「不合格」を他の全復号者装置へ通知し、不正者を排除する（Ｓ９）。

[0053]
After all decoding person apparatus disperse Vj with the above-mentioned procedure, each decoding person's Pj apparatus, vj and b_{0j}
It transmits to all other decoding person apparatus through a broadcast type communication channel (S7).
The apparatus of each decoding person Pj who received this checks that $C_{0j}=g1^{Vj}h^{b0j} \bmod p$ is formed, and verifies Vj (S8).
When not formed, it notifies a "rejection" to other all decoding person apparatus like the above, it eliminates an irregular person (S9).

【００５４】
正しいと確認された全てのＶｋから任意に２ｔ＋１個を選択し（Ｓ１０）、指数部に対する秘密

[0054]
If correct, it will choose 2t+1 piece from all checked Vk(s) as desired (S10), and it examines whether the value V decompressed

復元手順により復元した値Ｖが１に等しいか否かを調べる（Ｓ１１）。指数部に対する秘密復元手順は文献 Cramer,et.al: " A seure and Optimally Efficient Multi-Authority Election Scheme " , Advances in Cryptology-Eurocrypt'97 , LNCS 1233 Springer-Verlag, pp.103-118, 1997 に詳しい。以下に、選択した２ｔ＋１個のＶｋのインデックスｋの集合をαとした場合の指数部に対する復元手順を示す。指数部の秘密値はＰｅｄｅｒｓｅｎの検証可能秘密分散法で得られた秘密値であるとする。

with the secret decompression procedure with respect to an index part is equal to 1 (S11).
The secret decompression procedures with respect to an index part are documents. Cramer, et.al: "A seure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-Eurocrypt'97, LNCS 1233 Springer-Verlag, pp.103-118, and 1997 It is detailed.
The decompression procedure with respect to the index part at the time of making into (alpha) an ensemble of the index k of 2t+1 piece Vk chosen as below is shown.
The secret value of an index part presupposes that it is the secret value acquired with the verifiable secret dispersion method of Pedersen.

【００５５】

[0055]

Ｒ－１）まず、Ｌａｇｒａｎｇｅ補間係数を

R-1) IT IS LAGRANGE INTERPOLATION COEFFICIENT FIRST.

【００５６】

[0056]

【数１】

[EQUATION 1]

$$\lambda_{j,\alpha} = \Pi_{k \in \alpha,\ k \neq j} j/(j-k)$$

として計算する。

It calculates as these.

Ｒ－２）次に、

R-2) NEXT,

【００５７】

[0057]

【数２】

$$V=\Pi_{j\in\alpha}\ V_j^{\lambda j,\alpha}\ \mathrm{mod}\ p$$

[EQUATION 2]

を計算する。Ｖが１でないならば他の２ｔ＋１個の組み合わせで同様に秘密復元手順を繰り返す（Ｓ１２）。全ての組み合わせについていずれも復元値が１に等しくないならば、不合格を通知して停止する。

It calculates these.
If V is not 1, it will repeat a secret decompression procedure similarly in other 2t+1 piece combination (S12).
About all combination, if the decompression value is not all equal to 1, it will notify a rejection and will stop.

【００５８】
一つでも１になる組み合わせがあったならば、この暗号文を合格とする。各復号者Ｐｊの装置は図４に示すようにＤｊ＝ｕ１^{zj}mod ｐを計算し（Ｓ１）、放送型通信路により他の全ての復号者装置へ送信する（Ｓ２）。Ｄｊを受信した各復号者装置はＤ１，…，ＤｎのＵ１を底とする離散対数がＢＣＨ符号のコードワードであることを確認し（Ｓ４）、コードワードであれば、前述の指数部に対する秘密復元手順によりＤ＝ｕ１^{z} mod ｐを復元し（Ｓ５）、ｍ＝ｅ／Ｄ mod ｐを計算してメッセージｍを復号する（Ｓ６）。ステップＳ４でコードワードでなければ、零知識証明により、計算の正しさを証明させ、証明できないものは

[0058]
If there is combination set to 1 at least one, it will consider this cryptogram as a pass.
As shown in FIG. 4, each decoding person's Pj apparatus calculates Dj=u1^{zj}mod p, and transmits it to all other decoding person apparatus according to (S1) and a broadcast type communication channel (S2).
Each decoding person apparatus which received Dj
By checking that the discrete logarithm which uses u1 of D1...,Dn as a bottom is the coding word of a BCH code, if it is (S4) and the coding word, it will decompress D=u1^{z} mod p with the secret decompression procedure with respect to the above-mentioned index part, it will calculate (S5) and m=e/D modp, and will decode Message m (S6).
If it is not the coding word in step S4, it will prove the rightness of calculation by zero knowledge proof.

不正のＤｉとして廃棄する（Ｓ７）。

It aborts the thing which cannot be proved as irregular Di (S7).

【実施例３】

以下に、この発明の第三の実施例について説明する。

[EXAMPLE 3]

Below, it demonstrates the 3rd Example of this invention.

【００５９】

各々の復号者装置間には、安全な通信路があるものとし、また、各復号者装置は、他の全員の復号者装置が同一の内容を受信することが保証される放送型通信路を利用できるものとする。大きな素数ｐ，ｑがあり、ｑはｐ－１を割り切るものとする。Ｇｑの元ｇ１，ｇ２をランダムに選択する。まず、ｎ人の復号者をＰ１～Ｐｎとし、各復号者Ｐｊに対し、固有の公開値ｗｊを割り振る。３ｔ＜ｎを満たすしきい値ｔを定める。

[0059]

That a safe communication channel shall be between each decoding person apparatus, and each decoding person apparatus receives the content with all the members' same other decoding person apparatus shall utilize the broadcast type communication channel guaranteed.

There are big prime numbers p and q.

Q shall give a clear-cut solution to p-1.

It chooses the origin g1 and g2 of Gq at random.

First, it sets n persons' decoding person to P1-Pn, and assigns the inherent open value wj to each decoding person Pj.

It defines threshold-value t which fills 3 t<n.

【００６０】

まず、Ｐｅｄｅｒｓｅｎによる秘密分散方法を示す。まず、ｇ，ｈを $\log_g h$ が未知であるようなＧｑの元とする。秘密値ａ０，ｂ０を分散する分配者Ｐの装置は、Ｚｑ上のｔ次の二つの多項式ｆ（Ｘ）＝ａ０＋ａ１Ｘ＋…＋ａｔX^t，ｇ（Ｘ）＝ｂ０＋ｂ１Ｘ＋…＋ｂｔX^tをａ０を除いてランダムに選択し、各受信者Ｐｊの装置へｆ（ｗｊ），ｇ（ｗ

[0060]

First, the secret dispersion method by Pedersen is shown.

First, it carries out g and h the origin of Gq whose $\log_g h$ is unknown.

The apparatus of the portioner P who disperses the secret values a0 and b0 are the t-th two polynomial $f(X)=a0+a1X+...+atX^t$ on Zq, except for a0, it chooses $g(X)=b0+b1X+...+btX^t$ at random, and sends f (wj) and g (wj) to the apparatus of each receiving party Pj through a safe communication channel.

ｊ）を安全な通信路を通じて送付する。

【００６１】
つぎに、各係数のコミット値Ｅｉをｉ＝０，…，ｔに対してＥｉ＝ｇ^{ai}ｈ^{bi}ｍｏｄ ｐのように計算し、放送型通信路を介して公開する。これらを受信した各Ｐｊの装置は、ｕｊｉ＝ｗｊ^{i}ｍｏｄ ｑとしてｇ$^{f(wj)}$ ｈ$^{g(wj)}$ ＝Ｅ０^{uj0} Ｅ１^{uj1} …Ｅｔ^{ujt} ｍｏｄ ｐが成り立つことを検証する。このＥ０^{uj0} Ｅ１^{uj1} …Ｅｔ^{ujt} ｍｏｄ ｐの値をＰｊの分散秘密値に対するコミットメントと呼ぶ。各係数のコミット値が公開されていれば、誰でも、どのＰｊの分散秘密値に対するコミットメントも計算することができる。

[0061]
Next, it calculates the commitment value Ei of each coefficient like Ei=g^{ai}h^{bi}mod p to i= 0..., t, and opens to the public through a broadcast type communication channel.
Each apparatus of Pj which received these verifies that g$^{f(wj)}$ h$^{g(wj)}$ =E0^{uj0} E1^{uj1} ...Et^{ujt} mod p is formed as uji=wj^{i} mod q.
It calls the value of this E0^{uj0} E1^{uj1} ...Et^{ujt} mod p the commitment with respect to the distributed secret value of Pj.
If the commitment value of each coefficient is exhibited, anyone can also calculate the commitment with respect to which distributed secret value of Pj.

【００６２】
以下では、この秘密分散方法をＰｅｄ（ａ０，ｂ０）［ｇ，ｈ］→ （ａ０ｊ，ｂ０ｊ）（Ｅ０，…，Ｅｔ）
のように書く。（ａ０，ｂ０）は分散される秘密情報であり、（ａ０ｊ，ｂ０ｊ）は各Ｐｊの装置が安全な通信路を介して受信する分散秘密値であり、それぞれｆ（ｗｊ），ｇ（ｗｊ）に等しい。（Ｅ０，…，Ｅｔ）は放送型通信路を通じて公開される、各係数のコミット値である。［ｇ，ｈ］はコミットを作成する際に用い

[0062]
Below, it is this secret dispersion method.
Ped (a0, b0) [g, h] -> (a0j, b0j) (E0..., Et)
It writes like these.
(a0, b0) are confidential informations dispersed.
(a0j, b0j) are distributed secret values which it receives through a communication channel with each safe apparatus of Pj.
It is equal to f (wj) and g (wj) respectively.
(E0..., Et) are commitment values of each coefficient exhibited through a broadcast type communication channel.
[g, h]
express the bottom which it uses when making a commitment.

る底を表す。上記記法に関して、特に断りがない限り、定数項を除く多項式の係数はランダムに選ぶものとする。

It is related with the above-mentioned account method.
Specifically, as long as there is no notice, it shall choose the coefficient of the polynomial except an absolute term at random.

【００６３】

このようにして分散された秘密値から、多項式補間によって元の秘密を回復する場合には、まず、各分散秘密値の保持者は、その値を公開する。公開された（ａ０ｊ，ｂ０ｊ）値に対して、$g^{a0j} h^{b0j} = E0^{uj0} E1^{uj1} \cdots Et^{ujt} \bmod p$ が成り立つことを確認する。この式が成り立つような任意のｔ＋１個の（ａ０ｊ，ｂ０ｊ）について、そのインデックスｊが作る集合をαとする。Ｌａｇｒａｎｇｅ補間係数を

[0063]

Thus, from the dispersed secret value, when a polynomial interpolation recovers the original secret, the holder of each distributed secret value exhibits the value first.
It checks that $g^{a0j} h^{b0j} = E0^{uj0} E1^{uj1} \ldots Et^{ujt} \bmod p$ is formed to the exhibited value (a0j, b0j).
Let the ensemble which the index j makes be (alpha) about t+1 (a0j as desired, b0j) of which this equation consists.
Lagrange interpolation coefficient

【００６４】

[0064]

【数３】

[EQUATION 3]

$$\lambda_{i,\alpha} = \Pi_{k \in \alpha,\ k \neq i}\, i/(i-k) \bmod q$$

とすると、

When it carries out,

【００６５】

[0065]

【数４】

[EQUATION 4]

$\Sigma_{j\in\alpha}\lambda_{j,\alpha}\ a0j \bmod q = a0$

となり、ａ０を回復することができる。ｂ０も同様にして回復できる。上記秘密分散方法は、底を一つだけ用いても全く同様に実行することができる。そのような場合は、Ｐｅｄ（ａ０）［ｇ］→（ａ０ｊ）（Ｅ０，…，Ｅｔ）と書く。

A these next door, a0 is recoverable.
B0 is recoverable similarly.
Even if it uses only one bottom, it can completely perform the above-mentioned secret dispersion method similarly.
In such a case
Ped(a0) [g] It writes it as -> (a0j) (E0..., Et).

【００６６】
この秘密分散方法を利用して、複数人が協調して分散された乱数を生成することができる。まず、Ｐｉの装置は、乱数ａｉ，ｂｉをＺｑより選択し、これをＰｅｄ（ａｉ，ｂｉ）［ｇ，ｈ］→（ａｉｊ，ｂｉｊ）（Ｅｉ０…，Ｅｉｔ）
のように分散する。Ｐ１～Ｐｎの全員がこれを実行する。すると、Ｐｊの装置は、（ａ１ｊ，ｂ１ｊ），…，（ａｎｊ，ｂｎｊ）を安全な通信路から受信し、（Ｅ１０，…，Ｅ１ｔ），…，（Ｅｎ０，…，Ｅｎｔ）を放送型通信路から受信する。このとき、Ｐｊの分散秘密値（ｘ１ｊ，ｘ２ｊ）を、ｘ１ｊ＝ａ１ｊ＋…＋ａｎｊ mod ｑ，ｘ２ｊ＝ｂ１ｊ＋…＋ｂｎｊ mod ｑとする。この分散秘密値から回復される乱数値ｘ１は、

[0066]
The random number dispersed in cooperation by two or more persons is generable using this secret dispersion method.
First, the apparatus of Pi chooses random numbers ai and bi from Zq, this
Ped(ai,bi)[g,h]->(aij,bij)(Ei0...,Eit)
It disperses like these.
All the members of P1-Pn perform this.
Then, the apparatus of Pj receives (a1j, b1j)..., (anj, bnj) from a safe communication channel, it receives (E10..., E1t)..., (En0..., Ent) from a broadcast type communication channel.
At this time, it sets the distributed secret value (x1j, x2j) of Pj to x1j=a1j+...+anj modq,x2j=b1j+...+bnj modq.
The random-number value x1 recovered from this distributed secret value,

【００６７】

【数５】

$$x1 = \Sigma_{j \in \alpha} \lambda_{k,\alpha} x1j = a1 + \cdots + an \mod q$$

であり、回復が実行されるまでは、誰にもその値が知られることはない。また、この秘密乱数値を定数とする多項式のｋ次の係数のコミット値ＥＸｋは、ＥＸｋ＝Ｅ１ｋ・Ｅ２ｋ…Ｅｎｋ mod ｐとなる。特に、ＥＸ０＝$g^{x1}h^{x2}$mod ｐであることに注意。この方法を、分散乱数生成とよび、
Ｒａｎｄ（[ａ]，[ｂ]）[ｇ，ｈ]→（ａｊ，ｂｊ）（Ｅ０，…，Ｅｔ）
と書く。（[ａ]，[ｂ]）は、生成される乱数値であり、[　]はその値がどの計算者に対しても未知であることを意味する。[ｇ，ｈ]，（ａｊ，ｂｊ）および（Ｅ０，…，Ｅｔ）の意味は、前述の秘密分散の記法と同様である。

[0067]

[EQUATION 5]

They are these.
The value is known by nobody until recovery is performed.
Moreover, the commitment value EXk of the k-th coefficient of the polynomial which makes this secret random-number value a constant constitutes EXk=E1 k-E2 k...Enkmod p.
Particularly, it is cautious of it being EX0=$g^{x1}h^{x2}$mod p.
It calls this method distributed random-number generation, rand([a], [b]) [g, h] -> (aj, bj) (E0..., Et)
It writes.
([a], [b]) are random-number values formed.
[ ]
means that the value is unknown to every accountant.
The implication of [g,h],(aj,bj) and (E0...,Et) is the same as that of the account method of above-mentioned secret dispersion.

【００６８】
全復号者装置は、しきい値ｔの分散乱数生成手順を
Ｒａｎｄ（[ｘ１]，[ｘ２]）[ｇ１，ｇ２]→（ｘ１ｊ，ｘ２ｊ）

[0068]
All decoding person apparatus are the distributed random-number generation procedures of threshold-value t.
Rand([x1], [x2]) [g1, g2] -> (x1j, x2j) (EX0...,

（ＥＸ０，…，ＥＸｔ）Ｒａｎｄ（[ｙ１]，[ｙ２]）[ｇ１，ｇ２]→（ｙ１ｊ，ｙ２ｊ）（ＥＹ０，…，ＥＹｔ）Ｒａｎｄ（[ｚ１]）[ｇ１]→（ｚ１ｊ）（ＥＺ０，…，ＥＺｔ）

EXt) Rand([y1], [y2]) [g1, g2] -> (y1j, y2j) (EY0..., EYt) Rand ([z1]) [g1] -> (z1j) (EZ0..., EZt)

のように３回実行し、復号者Ｐｊは秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）を得、これを復号者Ｐｊの秘密鍵とする。また、$Xj=g1^{x1j}g2^{x2j} \bmod p$，$Yj=g1^{y1j}g2^{y2j} \bmod p$，$Zj=g1^{zj} \bmod p$なる（Ｘｊ，Ｙｊ，Ｚｊ）を復号者Ｐｊの公開鍵とする。さらに、$X=EX0=g1^{x1}g2^{x2} \bmod p$，$Y=EY0=g1^{y1}g2^{y2} \bmod p$，$Z=EZ0=g1^{z} \bmod p$を暗号化手順に用いる公開鍵とする。ここで（ｘ１，ｘ２，ｙ１，ｙ２，ｚ）$\in Zq^5$は任意のｔ＋１組の秘密値（ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊ）から、秘密復元手順により復元される乱数である。

It performs 3 times like these, the decoding person Pj acquires a secret value (x1 j, x2 j, y1 j, y2 j, zj), let this be the decoding person's Pj secret key.
Moreover, let $Xj=g1^{x1j}g2^{x2j} \bmod p$, $Yj=g1^{y1j}g2^{y2j} \bmod p$, and $Zj=g1^{zj} \bmod p$ be the decoding person's Pj public key (Xj, Yj, Zj).
Furthermore, let $X=EX0=g1^{x1}g2^{x2} \bmod p$, $Y=EY0=g1^{y1}g2^{y2} \bmod p$, and $Z=EZ0=g1^{z} \bmod p$ be the public key which it uses for an encryption procedure.
(element of)(x1, x2, y1, y2, z) Zq^5 is a random number decompressed by a secret decompression procedure from t+1 set of secret values (x1 j, x2 j, y1 j, y2 j, zj) as desired here.

【００６９】
全復号者装置は、分散乱数生成手順Ｒａｎｄ（[ｒ]，[ｓ]）[ｇ１，ｇ２]→（ｒｊ，ｓｊ）（Ｒ０，…，Ｒｔ）を実行し、分散された乱数ｒ∈Ｚｑを生成し、各復号者Ｐｊの装置は秘密値ｒｊ，ｓｊを保持する（図６、Ｓ１）。ここでＲをＲ＝Ｒ０＝ｇ１

[0069]
All decoding person apparatus perform distributed random-number generation procedure Rand ([r], [s]) [g1, g2] -> (rj, sj) (R0..., Rt), it forms dispersed random-number r(element of)Zq, each decoding person's Pj apparatus maintains the secret values rj and sj (FIG. 6, S1).
It makes R into $R=R0=g1^{r}g2^{s} \bmod p$ here.

$^{r}g2^{s} \bmod p$とする。

【００７０】
次に、全復号者装置は、分散乗算手段によって秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′を得る（Ｓ２）。ここで、秘密値ｘ１ｊ′は、乱数ｒと秘密鍵ｘ１の積をしきい値ｔの秘密分散法により分散して得られる値であり、任意のｔ＋１人の復号者が持つｘ１ｊ′から、ｒｘ１（mod ｑ）を復号することが可能である。秘密値ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′についても同様に、それぞれ任意のｔ＋１個の値から、ｒｘ２（mod ｑ），ｒｙ１（mod ｑ），ｒｙ２（mod ｑ）を復元することができる。このような分散乗算手段については、以下のように実行する。

[0070]
Next, all decoding person apparatus obtain secret value x1j', x2j', y1j', and y2j' by distributed multiplication means (S2).
Here, secret value x1j' is a value obtained by dispersing the product of a random number r and a secret key x1 with the secret dispersion method of threshold-value t.
From x1j' which t+1 person's decoding persons as desired have, it can decode rx1 (mod q).
It can decompress rx2 (mod q), ry1 (mod q), and ry2 (mod q) from the values of t+1 piece respectively as desired similarly about secret value x2j', y1j', and y2j'.
About such distributed multiplication means, it performs as follows.

【００７１】
復号者Ｐｊの装置は、
Ｐｅｄ（ｘ１ｊ，ｘ２ｊ）[ｇ１，ｇ２]→（ｘ１ｊｉ，ｘ２ｊｉ）（ＥＸｊ０，…，ＥＸｊｔ）
を実行する。各Ｐｊの装置は、$Rj=g1^{rj}g2^{sj} \bmod p$を計算する。この値Ｒｊは、$uji=wj^{i} \bmod q$として$Rj=R0^{uj0}R1^{uj1}\cdots Rt^{ujt} \bmod p$のように計算しても良いので、誰でも計算できることに注意。

[0071]
The decoding person's Pj apparatus, ped(x1j, x2j) [g1, g2] -> (x1ji, x2ji) (EXj0..., EXjt)
It performs these.
Each apparatus of Pj calculates $Rj=g1^{rj}g2^{sj} \bmod p$.
Since this value Rj may be calculated like $Rj=R0^{uj0}R1^{uj1}\ldots Rt^{ujt} \bmod p$ as $uji=wj^{i} \bmod q$, it cautions it about the ability of anyone to calculate.

【００７２】

[0072]

次に、Ｐｊの装置は、Ｐｅｄ（ｘ１ｊ，ｘ２ｊ）でｘ１ｊ，ｘ２ｊを分散するのに用いた多項式をそのまま用いて、Ｐｅｄ（ｘ１ｊ，ｓ１ｊ）［Ｒｊ，ｇ２］→（ｘ１ｊｉ，ｓ１ｊｉ）（ＥＲＸ１ｊ０，…，ＥＲＸ１ｊｔ）
Ｐｅｄ（ｘ２ｊ，ｓ２ｊ）［Ｒｊ，ｇ２］→（ｘ１ｊｉ，ｓ２ｊｉ）（ＥＲＸ２ｊ０，…，ＥＲＸ２ｊｔ）
を実行する。ただし、ｓ１ｊ，ｓ２ｊはランダムに選び、また、これらを定数項とする多項式もランダムに選ぶ。

Next, the polynomial used for dispersing x1j and x2j by Ped (x1j, x2j) is used for the apparatus of Pj as it is, and it is Ped(x1j, s1j) [Rj, g2] -> (x1ji, s1ji) (ERX 1j0..., ERX1jt).
Ped(x2j, s2j) [Rj, g2] -> (x1ji, s2ji) (ERX 2j0..., ERX2jt)
It performs these.
However, s1j and s2j also choose at random the polynomial which chooses at random and makes these an absolute term.

【００７３】
最後に、Ｐｊの装置は
Ｐｅｄ（ｘ１ｊ・ｒｊ，ｘ１ｊ・ｓｊ＋ｓ１ｊ）［ｇ１，ｇ２］→（ｒｘ１ｊｉ，ｒｓ１ｊｉ）（ＥＲＸ１ｊ０，…，ＥＲＸ１ｊｔ）
Ｐｅｄ（ｘ２ｊ・ｒｊ，ｘ２ｊ・ｓｊ＋ｓ２ｊ）［ｇ１，ｇ２］→（ｒｘ２ｊｉ，ｒｓ２ｊｉ）（ＥＲＸ２ｊ０，…，ＥＲＸ２ｊｔ）
とする。

[0073]
To the last, it is the apparatus of Pj.
Ped(x1 j-rj, x1 j-sj+s 1j) [g1, g2] -> (rx1ji, rs1ji) (ERX 1j0..., ERX1jt)
Ped(x2 j-rj, x2 j-sj+s 2j) [g1, g2] -> (rx2ji, rs2ji) (ERX 2j0..., ERX2jt)
It carries out.

【００７４】
上記手順をＰ１～Ｐｎの各装置が実行する。Ｐｉの装置は、受信した分散秘密値の集合（ｒｘ１１ｉ，…，ｒｘ１ｎｉ）から、Ｌａｇｒａｎｇｅ補間係数を

[0074]
Each apparatus of P1-Pn performs the above-mentioned procedure.
The apparatus of Pi is the ensemble (rx 11i..., rx1ni) of a distributed secret value which received to a Lagrange interpolation coefficient.

【００７５】

[0075]

【数６】 [EQUATION 6]

$\lambda_{j,\alpha} = \Pi_{k\in\alpha,\ k\neq j} j/(j-k)$ として、

$x1j' = \Sigma_{j\in\alpha}\lambda_{j,\alpha}\ rx1jj \mod q$

As (lambda)j1 (alpha)=IIk□(alpha), k not equal to jj/(j-k),

を計算する。正しいｘ１ｊ′のインデックスの集合をβとし、｜β｜＞＝ｔ＋１のとき、

It calculates these.
Let an ensemble of the index of correct x1j' be (beta), | At the time of (beta)|>=t+1

【００７６】 [0076]

【数７】 [EQUATION 7]

$\Sigma_{j\in\beta}\lambda_{j,\beta}\ x1j' = \Sigma_{j\in\beta}\{\lambda_{j,\beta}\ \Sigma_{i\in\alpha}\lambda_{i,\alpha}\ rx1ij\}$

$= \Sigma_{i\in\alpha}\lambda_{i,\alpha}\ \{\Sigma_{j\in\beta}\lambda_{j,\beta}\ rx1ij\}$

$= \Sigma_{i\in\alpha}\lambda_{i,\alpha}\ ri\cdot x1i = r\cdot x1$

となり、乗算結果ｒ・ｘ１を回復することができるので、ｘ１ｊ′がｒ・ｘ１のｔ次の分散秘密値であることが分かる。ｘ１ｊ′と同様に、ｘ２ｊ′も計算する。更に、秘密値ｙ１ｊ′，ｙ２ｊ′についても同様に分散乗算手順を実行して計算する。

A these next door, multiplication result r-x1 is recoverable, therefore, it turns out that x1j' is the t-th distributed secret value of r-x1.
It calculates x2j' as well as x1j'.
Furthermore, it performs and calculates a distributed multiplication procedure similarly about secret value y1j' and y2j'.

【００７７】 [0077]

Cramer-Shoup 暗号方法により暗号化された平文ｍに対する暗

After receiving cryptogram E=(u1,u2,v,e) with respect to plaintext m enciphered by the

号文Ｅ＝（ｕ１，ｕ２，ｖ，ｅ）を受信した後（Ｓ３）、各復号者Ｐｊの装置は、ｃ＝Ｈ（ｕ１，ｕ２）およびＶｊ＝ｕ１$^{x1j+cy1j}$ ｕ２$^{x2j+cy2j}$ ｖ$^{-rj}$ mod ｐを計算し（Ｓ４）、放送型通信路を通じて他の全ての復号者装置へＶｊを送信する（Ｓ５）。次に、各復号者装置は、（Ｖ１，…，Ｖｎ）の指数部がＢＣＨ符号のコードワードであることを確認する（Ｓ６）。コードワード確認手順は、文献 F.J. MacWilliams : “ The Thory of Error Correcting Codes ” , North-Holland Mathematical Library, pp.201-202 または、M.Ben-Or,S.Goldwasser, A.Wigerson: “ Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation ” , 20th ACM Symposium on Theory of Computing, pp.1-10, 1988 に詳しい。以下にコードワード確認手順を示す。

・ｗ≠１を mod ｑでの１のｎ乗根とし、ξｉｊ＝ｗ$^{j(i-1)}$ mod ｑとする。

・ｊ＝１，…，２ｔの全てのｊについて

Cramer-Shoup cryptographic method, the apparatus of (S3) and each decoding person Pj calculates c=H(u1,u2) and Vj=u1$^{x1j+cy1j}$u2$^{x2j+cy2j}$v^{-rj} mod p.

(S4), it transmits Vj to all other decoding person apparatus through a broadcast type communication channel.

(S5).

Next, each decoding person apparatus checks that the index part of (V1..., Vn) is the coding word of a BCH code.

(S6).

Coding word check procedure, documents F.J. MACWILLIAMS : "THE THORY OF ERROR CORRECTING CODES", NORTH-HOLLAND MATHEMATICAL LIBRARY, PP.201-202

Or

M.Ben-Or,S.Goldwasser, a.Wigerson: ""< Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Comput

It is detailed to ation", 20 th ACM Symposium on Theory of Computing>", pp.1-10, and 1988.

The coding word check procedure is shown below.

It considers it as n root of 1 in *w!=1 を mod q, it considers it as (xi)ij=w$^{j(i-1)}$ modq.

All j of *j=1...,2t

【００７８】

[0078]

【数８】

[EQUATION 8]

$V1^{\varepsilon 1j} V2^{\varepsilon 2j} \cdots Vn^{\varepsilon nj} \bmod p = 1$

となることを確認する。上記手順により、（Ｖ１，…，Ｖｎ）の指数部が正しくないことが判明した場合、各復号者Ｐｊの装置は、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$の計算結果であることをｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊに関する情報を漏らすことなく、零知識証明によって他の復号者装置に証明する（Ｓ７）。

It checks becoming these.
When it becomes clear with the above-mentioned procedure that the index part of (V1...,Vn) is not correct, it is each decoding person's Pj apparatus, without it leaks the information concerning that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$, and] x1j',x2j',y1j',y2j',rj, it proves to another decoding person apparatus by zero knowledge proof (S7).

【００７９】
この零知識証明は、以下のように実行する。ただし、以下のＰｊに対する手順の説明では、全ての変数に添字ｊが付くため、これを省いて説明する。まず、Ｐｊの保持する分散秘密値ｘ１′，ｘ２′，ｙ１′，ｙ２′，ｒに対して、ａ，ａ１，ａ２，ｂ１をある乱数として
$R = g1^{r} g2^{s} \bmod p$
$RX1 = ERX10 = R^{x1} g2^{a1} \bmod p$
$RX2 = ERX20 = R^{x2} g2^{a2} \bmod p$

$RY1 = ERY10 = R^{y1} g2^{b1} \bmod p$
$RY2 = ERY20 = R^{y2} g2^{b2} \bmod p$
Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，

[0079]
It performs this zero knowledge proof as follows.
However, by explanation of the procedure with respect to following Pj, since Subscript j is attached to all variables, it excludes and demonstrates this.
First, it is to distributed secret value x1' which Pj maintains, x2', y1', y2', and r considering a, a1, a2, and b1 as a certain random number.
$R=g1^{r}g2^{s} \bmod p$
$RX1=ERX10=R^{x1}g2^{a1} \bmod p$
$RX2=ERX20=R^{x2}g2^{a2} \bmod p$

$RY1=ERY10=R^{y1}g2^{b1} \bmod p$
$RY2=ERY20=R^{y2}g2^{b2} \bmod p$
It can acquire the values R, RX1, RX2, RY1,

^{b2}mod p
なるコミットメントの値Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を、分散乱数生成手段および、分散乗算手段で公開された係数のコミット値から、誰にでも得ることができる。

and RY2 of the becoming commitment from the commitment value of the coefficient exhibited with distributed random-number generation means and distributed multiplication means to anyone.

【００８０】
Ｐｊは乱数ｗ０をＺｑよりランダムに選択し、
Ｋ＝ｇ，Ｌ＝ｇ^{w0}mod ｐ
を他の復号者装置へ送付する。
他の復号者装置は、協力して
Ｒａｎｄ([ｅ０],[ｅ１])[Ｋ,Ｌ]→(ｅ０ｉ，ｅ１ｉ)(Ｅｅ０，…，Ｅｅｔ)

[0080]
Pj chooses a random number w0 from Zq at random, k=g, L=g^{w0}mod p
It sends these to another decoding person apparatus.
Another decoding person apparatus cooperates.
Rand([e0], [e1]) [K, L] -> (e0i, e1i) (Ee0..., Eet)

を実行し、Ｅｅ０＝Ｋ^{e0}Ｌ^{e1}mod ｐをＰｊの装置へ送付する。

It performs these, it sends Ee0=K^{e0}L^{e1}mod p to the apparatus of Pj.

【００８１】
Ｐｊの装置は乱数ｗ１～ｗ１８をＺｑよりランダムに選択し、
T_1＝ｇ$_1{}^{w1}$ｇ$_2{}^{w2}$ mod ｐ
T_2＝ｇ$_1{}^{w3}$ｇ$_2{}^{w4}$ mod ｐ
T_3＝ｇ^{w5}ｇ^{w6} mod ｐ

[0081]
The apparatus of Pj chooses random-number w1-w18 from Zq at random, t_1=$g_1{}^{w1}g_2{}^{w2}$ modp
T_2=$g_1{}^{w3}g_2{}^{w4}$ modp
T_3=$g^{w5}g^{w6}$ modp

T_4＝Ｒ^{w1}ｈ^{w7} mod ｐ
T_5＝Ｒ^{w2}ｈ^{w8} mod ｐ
T_6＝Ｒ^{w3}ｈ^{w9} mod ｐ
T_7＝Ｒ^{w4}ｈ^{w10}mod ｐ

T_4=$R^{w1}h^{w7}$ modp
T_5=$R^{w2}h^{w8}$ modp
T_6=$R^{w3}h^{w9}$ modp
T_7=$R^{w4}h^{w10}$modp

T_8＝ｇ^{w11} ｈ^{w12}mod ｐ
T_9＝ｇ^{w13} ｈ^{w14}mod ｐ
T_{10}＝ｇ^{w15} ｈ^{w16}mod ｐ

T_8=$g^{w11}h^{w12}$ mod p
T_9=$g^{w13}h^{w14}$ mod p
T_{10}=$g^{w15}h^{w16}$ mod p

$T_{11}=g^{w17}\ h^{w18} \bmod p$

$T_{12}=u1^{w11+cw15}u2^{w13+cw17}v^{-w5} \bmod p$
It calculates these, it sends to another decoding person apparatus.

$T_{11}=g^{w17}\ h^{w18} \bmod p$

$T_{12}=u1^{w11+cw15}u2^{w13+cw17}v^{-w5} \bmod p$
を計算して、他の復号者装置へ送付する。

【００８２】
他の復号者装置は分散秘密値を公開してｅ０，ｅ１を回復し、Ｐｊの装置へ送付する。Ｐｊの装置は、$Ee0=K^{e0}L^{e1} \bmod p$が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、Ｐｊの装置は

[0082]
Another decoding person apparatus exhibits a distributed secret value, and it recovers e0 and e1, it sends to the apparatus of Pj.
The apparatus of Pj checks that $Ee0=K^{e0}L^{e1} \bmod p$ is formed, it stops proof, when not formed.
It is the apparatus of Pj when this is formed.

$S1=w1+e0 \cdot x1 \bmod q$
$S2=w2+e0 \cdot x2 \bmod q$
$S3=w3+e0 \cdot y1 \bmod q$

$S4=w4+e0 \cdot y2 \bmod q$
$S5=w5+e0 \cdot r \bmod q$
$S6=w6+e0 \cdot a \bmod q$
$S7=w7+e0 \cdot a1 \bmod q$

$S8=w8+e0 \cdot a2 \bmod q$
$S9=w9+e0 \cdot b1 \bmod q$
$S10=w10+e0 \cdot b2 \bmod q$
$S11=w11+e0 \cdot r-x1 \bmod q$

$S12=w12+e0(a \cdot x1+a1) \bmod q$
$S13=w13+e0 \cdot r-x2 \bmod q$
$S14=w14+e0(a-x2+a2) \bmod q$
$S15=w15+e0 \cdot r-y1 \bmod q$

$S14=w14+e0(a\cdot x2+a2) \bmod q$
$S15=w15+e0\cdot r\cdot y1 \bmod q$

$S16=w16+e0(a\cdot y1+b1) \bmod q$
$S17=w17+e0 \text{ and } r-y2 \bmod q$
$S18=w18+e0(a-y2+b2) \bmod q$

を計算してＳ１～Ｓ１８およびｗ０を他の復号者装置へ送付する。他の復号者装置は、

It calculates these and sends S1-S18 and w0 to another decoding person apparatus.
Other decoding person apparatus,

$L=g^{w0} \bmod p$
$g_1^{s1} g_2^{s2}=T_1 X^{e0} \bmod p$
$g_1^{s3} g_2^{s4}=T_2 Y^{e0} \bmod p$
$g^{s5} h^{s6}=T_3 R^{e0} \bmod p$

$R^{s1} h^{s7}=T_4 (RX1)^{e0} \bmod p$
$R^{s2} h^{s8}=T_5 (RX2)^{e0} \bmod p$
$R^{s3} h^{s9}=T_6 (RY1)^{e0} \bmod p$
$R^{s4} h^{s10}=T_7 (RY2)^{e0} \bmod p$

$g^{s11} h^{s12}=T_8 (RX1)^{e0} \bmod p$
$g^{s13} h^{s14}=T_9 (RX2)^{e0} \bmod p$
$g^{s15} h^{s16}=T_{10} (RY1)^{e0} \bmod p$
$g^{s17} h^{s18}=T_{11} (RY2)^{e0} \bmod p$

^{e0}mod p

$u1^{S11+cS15}u2^{S13+cS17}v^{-S5} = T_{12}V^{e0}$mod p
が成り立つことを検証する。

$U1^{S11+cS15}u2^{S13+cS17}v^{-S5}=T_{12}V^{e0}$mod p
It verifies that these are formed.

【００８３】
上式は、Ｐｊの装置がＶ，Ｘ，Ｙ，Ｒ，ＲＸ１，ＲＸ２，ＲＹ１，ＲＹ２を正しく作成した場合にのみ成り立つので、一つでも成り立たない場合は検証を失敗とする（添字“ｊ”を省略した説明は以上)。証明に失敗した復号者Ｐｊの装置は逸脱者であると見なされ、逸脱者の秘密値ｘ１ｊ′，ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′，ｒｊを他の復号者装置が秘密値回復手順を用いて回復し、正しいＶｊの値を公開する。ここでの秘密値回復手順については、例えば、文献 A.Herzberg, et.al: “Proactive secret sharing or:How to cope with perpetual leakage”, Advances in Cryptology-CRYPTO'95,LNCS 963, pp.339-352, Springer-Verlag, 1995 に詳しい。その公開された正しいＶｊの値を含めて、正しい（Ｖ１，…，Ｖｎ）を得る。

[0083]
Since an above formula is formed only when the apparatus of Pj makes V,X,Y,R,RX1,RX2,RY1,RY2 correctly, when not formed at least one, it considers verification as failure (explanation which omitted the subscript "j" above).
It is considered that the apparatus of the decoding person Pj who failed in proof is a deviation person, another decoding person apparatus recovers a deviation person's secret value x1j',x2j',y1j',y2j',rj using a secret value recovery procedure, it exhibits the correct value of Vj.
About a secret value recovery procedure here
For example, documents
It is detailed to A.Herzberg, et.al: " Proactive secret sharing or:How to cope with perpetual leakage", Advances in Cryptology-CRYPTO'95,LNCS 963, pp.339-352, Springer-Verlag, 1995.
It includes the exhibited correct value of Vj, it obtains the correct (V1...,Vn).

【００８４】
（Ｖ１，…，Ｖｎ）の指数部が正しいことを確認した後、指数

[0084]
After the index part of (V1..., Vn) checks the correct thing, it decompresses a value V with

部に対する秘密復元手順により、値Ｖを復元する。各復号者装置はＶが１に等しいか否かを調べ、等しくないならば復号を拒否して停止する（Ｓ８)。等しいならば、図４の場合と同様に、各復号者Ｐｊの装置はＤｊ＝ｕ１^{zj}ｍｏｄｐを計算し、放送型通信路により他の全ての復号者装置へ送信し、Ｄｊを受信した各復号者装置は（Ｄ１，…，Ｄｎ）に対して（Ｖ１，…，Ｖｎ）に対して行ったのと同様のコードワードの検証を行い、不正を検出した場合には同様に零知識証明を行って逸脱者を特定し、正しいＤｊの値を秘密値回復手順を用いて回復する。

the secret decompression procedure with respect to an index part.
It examines whether each decoding person apparatus has V equal to 1, if not equal, it will refuse decoding and will stop.
(S8).
If these etc. come to be by carrying out, each decoding person's Pj apparatus will calculate Dj=u1^{zj}modp like the case of FIG. 4, it transmits to all other decoding person apparatus according to a broadcast type communication channel, each decoding person apparatus which received Dj performs verification of the coding word similar to having carried out by receiving to (D1..., Dn) (V1..., Vn), when irregularity is detected, it performs zero knowledge proof similarly and specifies a deviation person, it recovers the correct value of Dj using a secret value recovery procedure.

【００８５】
ここでの零知識証明は以下のように実行する。Ｐｊの装置は乱数ｄ０をＺｑよりランダムに選択し、
Ｗ＝ｇ$_1$，Ｑ＝ｇ$_1$^{d0} ｍｏｄｐ
を他の復号者装置へ送付する。
他の復号者装置は、協力して
Ｒａｎｄ（[ｃ２]，[ｃ３]）[Ｗ，Ｑ]→（ｃ２ｉ，ｃ３ｉ）（Ｅｃ０，…，Ｅｃｔ）

[0085]
It performs zero knowledge proof here as follows.
The apparatus of Pj chooses a random number d0 from Zq at random, w=g$_1$,Q=g$_1$ ^{d0} modp
It sends these to another decoding person apparatus.
Another decoding person apparatus cooperates.
Rand([c2], [c3]) [W, Q] -> (c2i, c3i) (Ec0..., Ect)

を実行し、Ｅｃ０＝Ｗ^{c2}Ｑ^{C3} ｍｏｄｐをＰｊの装置へ送付する。

It performs these, it sends Ec0=W^{c2}Q^{C3} modp to the apparatus of Pj.

【００８６】
Ｐｊの装置は乱数ｄ１，ｄ２をＺｑよりランダムに選択し、
$T_{12}=g_1^{d1} \bmod p$
$T_{13}=u1^{d1} \bmod p$
を計算して、他の復号者装置へ送付する。他の復号者装置は分散秘密値を公開してｃ２，ｃ３を回復し、Ｐｊの装置へ送付する。

[0086]
The apparatus of Pj chooses random numbers d1 and d2 from Zq at random, $t_{12}=g_1^{d1} \bmod p$
$T_{13}=u1^{d1} \bmod p$
It calculates these, it sends to another decoding person apparatus.
Another decoding person apparatus exhibits a distributed secret value, and it recovers c2 and c3, it sends to the apparatus of Pj.

【００８７】
Ｐｊの装置は$Ec0=W^{c2}Q^{C3} \bmod p$が成り立つことを確認し、成り立たない場合は証明を中止する。これが成り立つ場合、Ｐｊの装置は
$S0=d1+c2 \cdot z1 \bmod q$
を計算してＳ０およびｄ０を他の復号者装置へ送付する。他の復号者装置は、
$Q=g_1^{d0} \bmod p$

[0087]
The apparatus of Pj checks that $Ec0=W^{c2}Q^{C3} \bmod p$ is formed, it stops proof, when not formed.
It is the apparatus of Pj when this is formed.
S0=d1+c2 and z1mod q
It calculates these and sends S0 and d0 to another decoding person apparatus.
Other decoding person apparatus, $q=g_1^{d0} \bmod p$

$g_1^{s0}=T_{12}Xj^{c2} \bmod p$
$u1^{s0}=T_{13}Dj^{c2} \bmod p$
が成り立つことを検証する。

$G_1^{s0}=T_{12}Xj^{c2} \bmod p$
$U1^{s0}=T_{13}Dj^{c2} \bmod p$
It verifies that these are formed.

【００８８】
上式は、Ｐｊの装置がＤｊを正しく作成した場合にのみ成り立つので、一つでも成り立たない場合は検証を失敗とする。各復号者装置は、正しい（Ｄ１，…，Ｄｎ）から、指数部に対する秘密復元手順によって$D=u1^{z} \bmod p$を復元し、ｍ＝ｅ／Ｄ

[0088]
Since an above formula is formed only when the apparatus of Pj makes Dj correctly, when not formed at least one, it considers verification as failure.
From the correct (D1...,Dn), with the secret decompression procedure with respect to an index part, each decoding person apparatus decompresses $D=u1^{z} \bmod p$, calculates

mod ｐを計算してメッセージｍを復号する。

m=e/Dmod p, and decodes Message m.

【００８９】

図７に実施例２における復号者装置の機能構成例を示す。メモリ２１にはｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊの秘密鍵が記憶され、公開値ｗｊ，ｇ１，ｇ２，ｐ，ｑなども記憶され、更に外部へ送信する情報、外部から受信する情報を一時記憶するためにメモリ２１が用いられる。分散乱数生成部２２は秘密分散器２３、分散秘密検証器２４、分散秘密加算器２５よりなり、これらにより、秘密鍵ｘ１ｊ，ｘ２ｊ，ｙ１ｊ，ｙ２ｊ，ｚｊが作成され、また乱数ｒの分散値ｒｊも生成される。ハッシュ器２６により受信暗号文Ｅについてｃ＝Ｈ（ｕ１，ｕ２）のハッシュ関数演算が行われ、またべき乗演算器２７によりＶｊ＝（$u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1}$）^{rj}mod ｐの演算が行われる。秘密分散部３１は秘密分散器３２、分散秘密検証器３３よりなり、秘密値ＶｊがＶｊｋにしきい値２ｔの検証可能秘密分散法により分散される。指数部秘密復元器３４により、Ｖｋの指数部に対する秘密復元手順が実行され、ＢＣＨコードワード検証器３５によりＤ１，…，Ｄｎのｗ１を底とする離散対数がＢＣ

[0089]

The example of functional composition of the decoding person apparatus in Example 2 is shown in FIG. 7.

The secret key of x1j,x2j,y1j,y2j,zj is stored in memory 21, the open values wj, g1, g2, and p and q etc. are also stored, furthermore, memory 21 is used in order to carry out the temporary memory of the information which it transmits to the exterior, and the information which it receives from the outside.

The distributed random-number generation part 22 is made up of the secret dispersion device 23, a distributed secret verification device 24, and a distributed secret adder 25, and secret-key x1j,x2j,y1j,y2j,zj is made by these, and the distributed value rj of a random number r is also formed.

The hash function calculation of c=H (u1, u2) is performed about the receiving cryptogram E with the hash device 26, moreover, it is Vj= (the calculation of $u1^{x1j+cy1j}u2^{x2j+cy2j}v^{-1})^{rj}$mod p is performed.) by the power calculator 27.

The secret dispersion part 31 is made up of a secret dispersion device 32 and a distributed secret verification device 33, and the secret value Vj is dispersed by Vjk with a with a threshold value of 2t verifiable secret dispersion method.

With the index part secret decompression device 34, the secret decompression procedure with respect to the index part of Vk is performed, and it is checked that the discrete

H符号のコードワードであることが確認される。放送型通信受信器３６、放送型通信送信器３７、個別通信受信器３８、個別通信送信器３９が設けられ、更に制御部４１により各部が順次動作させられる。

logarithm which uses w1 of D1...,Dn as a bottom with the BCH coding word verification device 35 is the coding word of a BCH code.
The broadcast type communication receiver 36, the broadcast type communication transmitter 37, the individual communication receiver 38, and the individual communication transmitter 39 are provided, furthermore, the control part 41 lets each part carry out a sequential operation.

【００９０】

図８に実施例３に用いられる復号者装置の機能構成を、図７と対応する部分に同一番号を付けて示す。分散乗算手段４３により、乱数ｒと秘密鍵ｘ１の積をしきい値ｔの秘密分散法により分散した値ｘ１ｊ′、同様な値ｘ２ｊ′，ｙ１ｊ′，ｙ２ｊ′が求められる。証明部４４は乱数生成器４５、べき乗演算器４６、乗余乗算・加算器４７よりなり、Ｖｊが$u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$の計算結果であることを零知識証明によって他の復号者に証明する。零知識証明手順中の検証は検証部４８のべき乗演算器４９と比較器５１により行われる。

[0090]

The same number is numbered and shown in the part which corresponds the functional composition of the decoding person apparatus used for FIG. 8 at Example 3 with FIG. 7.
By the distributed multiplication means 43, value x1j' which dispersed the product of a random number r and a secret key x1 with the secret dispersion method of threshold-value t, similar value x2j', y1j', and y2j' are called for.
Proof part 44
Random-number generation device 45, power calculator 46, a remainder multiplication and adder 47
It is made up of these, it proves that Vj is the calculation result of $u1^{x1j'+cy1j'}u2^{x2j'+cy2j'}v^{-rj} \bmod p$ to another decoding person by zero knowledge proof.
Verification in zero knowledge proof procedure is performed by the power calculator 49 and comparator 51 of the verification part 48.

【００９１】

[0091]

【発明の効果】

Cramer-Shoup 暗号における復

[ADVANTAGE OF THE INVENTION]

Since the correctness of a cryptogram is

号時の検証式の値を、この発明では復号者の誰もがその値を知り得ない乱数によってべき乗した値が１となるか否かを検証することによって暗号文の正当性を検証しているため、べき乗した値を公開しても、本来の検証式における値に関する情報は一切漏洩しない。この値が正しく作成されたことを零知識証明によって第三者へ証明する事により、受信した暗号文が元の検証式を満足しないことを第三者へ証明することができる。

verified by verifying whether the value which carried out the power of the value of the verification type at the time of decoding in a Cramer-Shoup code with the random number with which everyone of a decoding person cannot know that value in this invention is set to 1, even if it exhibits the value which carried out the power, it reveals no information about the value in an original verification type.
By proving to a third person that this value was made correctly by zero knowledge proof, it can prove to a third person that the cryptogram which received does not satisfy the original verification type.

【００９２】

さらに、乱数でべき乗するという計算を分散計算により、全計算者の協力で行うことによって、検証式を満たさない場合にも、べき乗する前の検証式の値がどの復号者にも漏洩することはないため、復号者の中に不正者がいたとしても、攻撃者は何の利益も得ることができないため、選択的暗号文攻撃に対して安全なしきい値付き復号方法となっている。

[0092]

Since the value of the verification type before carrying out a power is not revealed to all the decoding person, either, also when not filling a verification type by furthermore performing calculation of carrying out a power by random numbers, by cooperation of all accountants by distributed calculation, even if there is an irregular person in a decoding person, since an aggressor can get no profits, he is the decoding method with a safe threshold value to the alternative cryptogram attack.

【００９３】

更にこの発明の別の観点によれば、零知識証明によって計算結果の正当性を各復号者に証明させることによって不正者を特定し、正当なデータのみを用いて暗号文の検証を行うため、復号

[0093]

Furthermore, according to another viewpoint of this invention, it specifies an irregular person by letting each decoding person prove the correctness of a calculation result by zero knowledge proof, since verification of a cryptogram is performed only using rightful

者の数ｎに比例した計算量で検証を行うことが可能である。また、各復号者の計算結果がＢＣＨ符号のコードワードとなるように各復号者の固有の公開値を定め、まず、計算結果がコードワードであることを受信者が検証し、コードワードでない場合にのみ零知識証明を実行することによって、正しい暗号文を受信した場合には、通信量を抑えたまま効率的な計算を行うことが可能である。

data, it can perform verification by the computational complexity proportional to several n of a decoding person.
Moreover, it sets each decoding person's inherent open value that each decoding person's calculation result constitutes the coding word of a BCH code, and a receiving party verifies first that a calculation result is the coding word, when the correct cryptogram is received by performing zero knowledge proof only when it is not the coding word, it can perform efficient calculation, with the amount of communication restrained.

【００９４】
さらに、不正者が特定された場合に、他の復号者が協力してその不正な復号者が持つ分散秘密鍵を算出し、公開することによって、だれもがその不正な復号者に代わって正しい結果を計算することができるようにすることによって、１／３以上の不正者が存在しても、それが１／２未満である限りにおいて、正しい検証結果および復号結果を得ることが可能である。

[0094]
Furthermore, another decoding person computes the distributed secret key which the irregular decoding person has in cooperation with the case where an irregular person is specified, although it also becomes bored by opening to the public, even if the irregular person more than 1/3 exists by enabling it to calculate the correct result instead of the irregular decoding person, as long as it is under 1/2, it can obtain the correct verification result and a decoding result.

【図面の簡単な説明】

[BRIEF DESCRIPTION OF THE DRAWINGS]

【図１】
この発明の実施例１のシステム構成を表す図。

[FIG. 1]
The figure showing the system assembly of Example 1 of this invention.

【図２】

[FIG. 2]

この発明の実施例１における復号者装置の検証動作手順を示す流れ図。

The flowchart showing the verification action procedure of the decoding person apparatus in Example 1 of this invention.

【図３】
この発明の実施例２のシステム構成を表す図。

[FIG. 3]
The figure showing the system assembly of Example 2 of this invention.

【図４】
この発明の実施例２における復号者Ｐｉの装置の復号動作手順を示す流れ図。

[FIG. 4]
The flowchart showing the decoding action procedure of the decoding person's Pi apparatus in Example 2 of this invention.

【図５】
この発明の実施例２における復号者Ｐｉの装置の検証動作手順を示す流れ図。

[FIG. 5]
The flowchart showing the verification action procedure of the decoding person's Pi apparatus in Example 2 of this invention.

【図６】
この発明の実施例３における復号者Ｐｉの装置の検証動作手順を示す流れ図。

[FIG. 6]
The flowchart showing the verification action procedure of the decoding person's Pi apparatus in Example 3 of this invention.

【図７】
実施例２における復号者装置の機能構成を示す図。

[FIG. 7]
The figure showing the functional composition of the decoding person apparatus in Example 2.

【図８】
実施例３における復号者装置の機能構成を示す図。

[FIG. 8]
The figure showing the functional composition of the decoding person apparatus in Example 3.

【図１】

[FIG. 1]

図1

FIG. 1

11 Cryptogram maker apparatus

12 Decoding person apparatus

13 Verification person apparatus

【図2】 [FIG. 2]

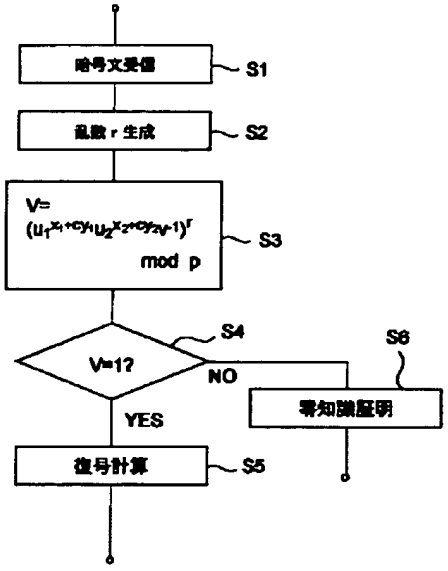

図2

FIG. 2

S1 Cryptogram reception

S2 Random-number r generation

S5 Decoding calculation
S6 Zero knowledge proof

【図３】 [FIG. 3]

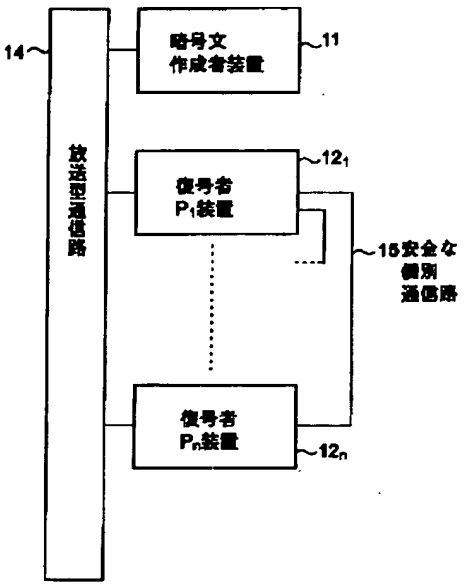

図３

FIG. 3
11 Cryptogram maker apparatus
121 Decoding person P1 apparatus
12n Decoding person Pn apparatus
14 Broadcast type communication channel
15 Safe individual communication channel

【図４】 [FIG. 4]

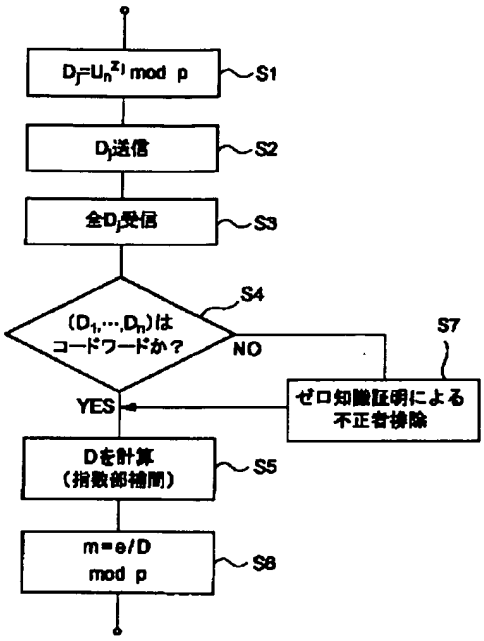

図4

FIG. 4

S2 Dj transmission

S3 All Dj reception

S4 Are (D1, ..., Dn) coding words?

S5 It calculates D (index part interpolation).

S7 Irregular person rejection by zero knowledge proof

【図5】 [FIG. 5]

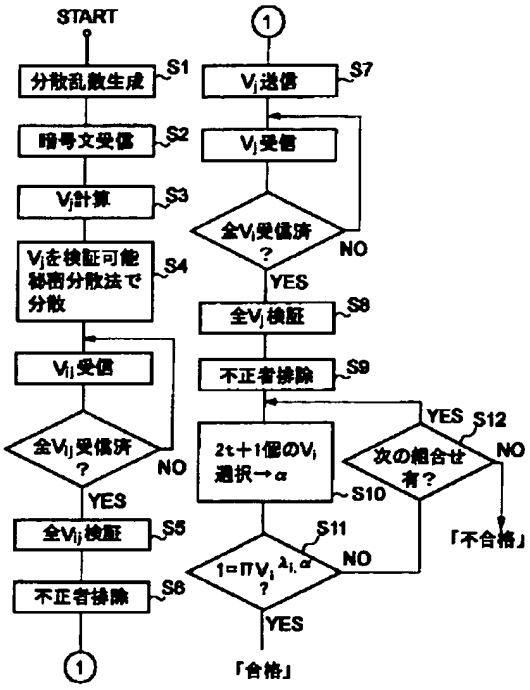

図 5

FIG. 5

START

S1 Distributed random-number generation

S2 Cryptogram reception

S3 Vj calculation

S4 It disperses Vj with verifiable secret dispersion method.

Vij reception

All Vij received ?

S5 All Vij verification

S6 Irregular person rejection

S7 Vj transmission

Vj reception

All Vj received ?

S8 All Vj verification

S9 Irregular person rejection

S10 Vi choice of 2t+1 piece -> (alpha)

Pass

S12 The following combination Present?

↓

Failure

【図６】 [FIG. 6]

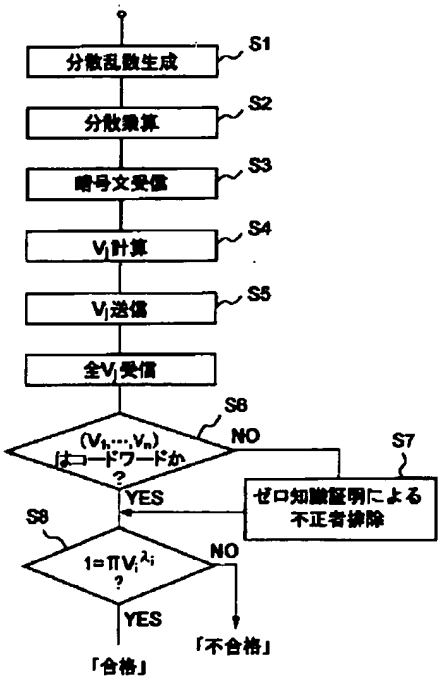

図６

FIG. 6

S1 Distributed random-number generation

S2 Distributed multiplication

S3 Cryptogram reception
S4 Vj calculation
S5 Vj transmission

All Vj reception

S6 (V1, ..., Vn) Is it coding word?
S7 Irregular person rejection by zero knowledge proof

Failure
Pass

【図７】 [FIG. 7]

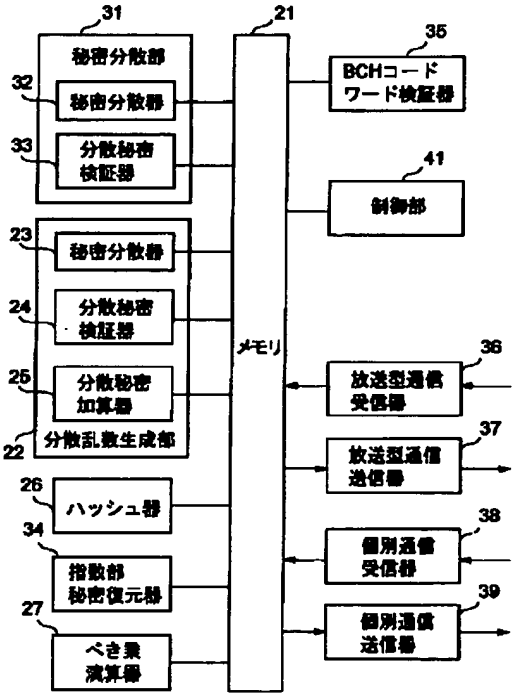

図７

FIG. 7

31 Secret dispersion part
32 Secret dispersion device
33 Distributed secret verification device

22 Distributed random-number generation part
23 Secret dispersion device
24 Distributed secret verification device
25 Distributed secret adder

26 Hash device
34 Index part secret decompression device
27 Power calculator

21 Memory

35 BCH coding word verification device
41 Control part
36 Broadcast type communication receiver
37 Broadcast type communication transmitter
38 Individual communication receiver
39 Individual communication transmitter

【図８】 [FIG. 8]

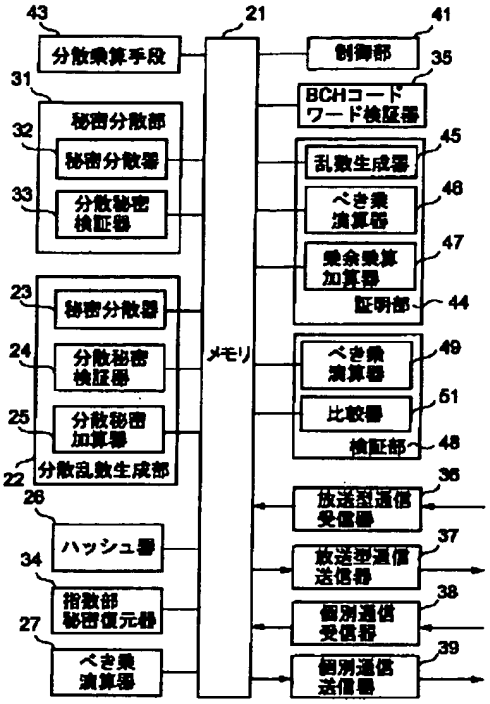

図8

43 Distributed multiplication means

31 Secret dispersion part
32 Secret dispersion device
33 Distributed secret verification device

22 Distributed random-number generation part
23 Secret dispersion device
24 Distributed secret verification device
25 Distributed secret adder

26 Hash device
34 Index part secret decompression device
27 Power calculator

21 Memory

41 Control part
35 BCH coding word verification device

45 Random-number generation device
46 Power calculator
47 Remainder multiplication adder
44 Proof part

49 Power calculator
51 Comparator
48 Verification part

36 Broadcast type communication receiver
37 Broadcast type communication transmitter
38 Individual communication receiver
39 Individual communication transmitter

THOMSON SCIENTIFIC TERMS AND CONDITIONS

Thomson Scientific Ltd shall not in any circumstances be liable or responsible for the completeness or accuracy of any Thomson Scientific translation and will not be liable for any direct, indirect, consequential or economic loss or loss of profit resulting directly or indirectly from the use of any translation by any customer.

Thomson Scientific Ltd. is part of The Thomson Corporation

Please visit our website: "www.THOMSONDERWENT.COM" (English)
"www.thomsonscientific.jp" (Japanese)